SANS DFIR CURRICULUM

FOUNDATION

- FOR108 Digital Forensic Foundations
- SEC504 Hacker Techniques, Exploits, and Incident Handling GCIH

IN-DEPTH

- FOR408 Windows Forensics GCFE
- FOR508 Advanced Incident Response GCFA
- FOR572 Advanced Network Forensics and Analysis
- FOR610 REM: Malware Analysis GREM

SPECIALIZATION

- FOR518 Mac Forensics
- FOR526 Memory Forensics In-Depth
- FOR585 Advanced Smartphone Forensics

SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

POSTER

SUMMER 2014 – 30TH EDITION

FOR585:

Advanced Smartphone Forensics

MOST RELEVANT EVIDENCE PER GIGABYTE!

digital-forensics.sans.org

MOST RELEVANT EVIDENCE PER GIGABYTE!

Nine Elements of Mobile Forensic Process

digital-forensics.sans.org/community/cheat-sheets

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

FILE SYSTEM
- Includes active files and folders from file system
- May contain remnants of deleted items
- Is supported for most devices by most tools
- Reporting may be more complex

PHYSICAL
- Includes active and deleted data
- Absolute vs. Records
- Not supported for all devices
- Reporting is generally more complex

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

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 and these devices CANNOT be accessed if the passcode is set and unknown
   - iphone 4S/5/5s/5c
   - ipod touch 5G
   - ipad 2/3/4/mini
3. Acquire supporting media
   - SIM card
4. Check associated computers and media for device backups
   - Check paired computers for lockdown.plist file
   - Check computers for iTunes backups

Android
1. Physical access requires that USB debugging mode is enabled. Forensic tools will use custom bootloaders to bypass the passcode if applicable
2. Acquire supporting media
   - SIM cards
   - 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

Knock-Off
1. Physical acquisition will most often bypass passcode

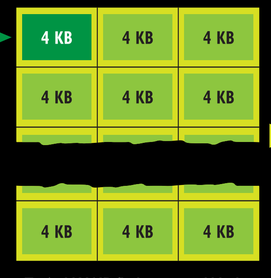
Device Is Off

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

If you cannot access the home screen for Nokia or Windows devices because the SIM card has been removed to prevent network access, attempt SIM ID cloning.

Defining the Memory Chip

Data written in 4 KB pages



Data erased in 256 KB blocks

64 writable pages in one erasable block

Typical NAND flash pages and blocks

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 & 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 downloads 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

MOBILE MALWARE DETECTION
- SIGNATURE BASED
- SPECIFICATION BASED
- BEHAVIORAL BASED
- DATA MINING
- CLOUD BASED

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
  - Dexter
  - Dex2jar
  - 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
  - Kaspersky
  - Symantec (Norton)
  - AVG
  - Lookout
  - TrendMicro
  - BitDefender
  - Sophos
  - TrustGo

Unpacking & Decompiling an Application File (.apk)

Preparation

- Install most recent version of Dex2Jar on your desktop: code.google.com/p/dex2jar/downloads/list
- Install most recent version of JD-GUI on your desktop: www.softpedia.com/get/Programming/Debuggers-Decompilers-Dissasemblers/JD-GUI.shtml
- Install most recent Java Development Kit: www.oracle.com/technetwork/java/javase/downloads/jdk7-downloads-1880260.html

Step 1

- RENAME the application (.apk) file, appending a .zip extension to the end of the file name.
  - EXAMPLE: zombie_highway.apk becomes zombie_highway.apk.zip

Step 2

- DOUBLE CLICK on the newly named .zip file in order to open it and see the contents of the file.
- Locate the classes.dex file within the unzipped file
- COPY the classes.dex file

Step 3

- PASTE the classes.dex file into the dex2jar directory created during the preparation stage
- OPEN a command prompt and navigate to the dex2jar directory on the desktop
- EXECUTE the batch file:
  - dex2jar.bat classes.dex
- This command will create a file named classes_dex2jar.jar in the dex2jar directory

Step 4

- OPEN the JD-GUI Java Decompiler and navigate to the classes_dex2jar.jar created in the previous step
- OPEN the classes_dex2jar.jar file in order to view and navigate the contents of the programming to reveal what the .apk file is doing

DFIR Smartphone Forensics

MOST RELEVANT EVIDENCE PER GIGABYTE!

SANS FOR585: Advanced Smartphone Forensics 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

10:15 AM 100%

FILES OF INTEREST	DESCRIPTION
mobile/Library/DataAccess	Account information used to set up apps (Email, #, etc)
Var/mobile/Library/Keyboard	dynamic-text.dat
DCIM/100APPLE Folder	User Created Photos
/private/mobile/var/applications	Application Folders
Media/PhotoData/*	Photos
Library/Cookies/Cookies.binarycookies	Safari activity
Library/Preferences/com.apple.assistant*	Siri
Library/Preferences/com.apple.imservice*	SMS, iMessage & FaceTime
Media/Recordings/*	Voice Memos
Library/Voicemail/*	Voicemail
Library/SpringBoard/LockBackgroundThumbnail.jpg	Wallpaper
Library/SpringBoard/HomeBackground.cpbitmap	Wallpaper
Library/SpringBoard/HomeBackgroundThumbnail.jpg	Wallpaper
Library/SpringBoard/LockBackground.cpbitmap	Wallpaper

DATABASE	DESCRIPTION
Library/CallHistory/call_history.db	Call logs
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/Calendar/Extras.db	Extras for Calendar
Library/Notes/notes.sqlite	Notes
Library/Safari/*	Safari activity
Library/Accounts/Accounts3.sqlite	Account information
Library/BulletinBoard/ClearedSections.plist	Logs of cleared notifications
Library/Caches/com.apple.WebAppCache/ApplicationCache.db	Website cache
Library/Keyboard/UserDictionary.sqlite	User created auto-correct
Library/Voicemail/voicemail.db	Voicemail

*Suggests reviewing all files for relevance

BlackBerry

DATABASE	EVIDENTIARY DATA
Address Book	Contacts along with contact picture if applicable
Attachment Data	Attachments viewed on the device
Auto Text	Dictionary for misspelled words
BBGroups	BlackBerry Messenger Groups
Browser Bookmarks	Bookmarked web pages
Browser URLs	Typed URLs (entered by user)
Folders	Message folders created by the user
Location-Based Services	Location tracking most often utilized by devices on BES
Messages	Messages on the device
MMS Messages	MMS message history
Phone Call Logs	Call log history
Phone History	More complete phone call history
PIN Messages	PIN Messages
Purged Messages	Information related to messages deleted from handset
RMS Databases	Information related to installed applications
Saved Email Messages	All saved Email messages on handset
SMS Messages	SMS message history

NOKIA

PATH	EVIDENTIARY DATA	FILE TYPES
C:\RESOURCE	Application associated files	.rsc
C:\RESOURCE\APPS	Application associated files	.r, .rsc
C:\RESOURCE\PLUGINS	Application associated files	.r, .rsc
C:\System\Install	Application installer files	.sis, .sisx
C:\System\Install\Registry	Application registry files	.reg
C:\DATA\Lifeblog\Lifeblog.db	Proprietary database containing lifeblog data paths along with cell tower IDS and geolocation information	.db
C:\DATA\Lifeblog\Database\Textindex.db	Proprietary database containing lifeblog data	.db
C:\DATA\Lifeblog\Notes	"Notes" posted to Lifeblog application	.txt
C:\Favourites\BrowserBookmarks\Favourites.db	Web browsing bookmarks	.db
C:\DATA\Images	User images	.3gp
C:\DATA\Videos	User videos	.jpg
C:\DATA\SOUNDS\DIGITAL	User audio	.acc, .wav
z:\resource	Application associated files	.r
z:\resource\apps	Application associated files	.r, .rsc, .mif
z:\resource\help	Application associated files	.h
z:\resource\messaging\mtm	Application associated files	.r
z:\resource\plugins	Application associated files	.r, .rsc, .dll55L
z:\system\install	Application installer files	.sis, .sisx
z:\Data\Sounds\Digital	Application audio files	.acc
z:\system\sounds\Digital	Application audio files	.acc, .wav
C:\Private\100012a5\DBS_100065FF_Contacts.cdb	Database holding contacts in the form of vcards (.vcf)	.cdb
C:\Private\1000484b\Mail	Message database (contains email, mms, sms, and bluetooth messages)	Folder
C:\Private\1000484b\Mail2	Message database (contains email, mms, sms & bluetooth messages	Folder
C:\Private\100012a5\DBS_102072I6_SWInstLog.db	Application install log	.db
C:\DATA\NEF\NEFConfig.xml	Configuration file containing handset IMEI (look for similar file on SD card to tie SD card to handset)	.xml

ANDROID

PARTITION	FILE	TABLE	DESCRIPTION
Data	Root/Property/persist.sys.timezone	*	Timezone
Data	Root/Property/netpolicy.xml	*	Timezone
Data	com.android.providers.contacts/contacts2.db	calls	Call logs
Data	com.android.providers.contacts/contacts2.db	accounts	Login info
Data	com.android.providers.contacts/contacts2.db	contacts & raw contacts	Contacts
Data	com.android.providers.telephony/mmssms.db	sms & part	SMS/MMS
Data	com.google.android.apps.maps/da_destination_history	destination history	Maps
Data	com.google.android.apps.maps/search_history.db	history & suggestions	Maps
Data	com.android.email/webviewCache.db	*	Internet History
Data	com.android.browser/databases/Browser.db	*	Internet History
Data	com.android.browser/databases/webview.db	*	Internet History
Data	com.android.browser/databases/webviewCache.db	*	Internet History
Data	com.android.browser/app_databases/http_www.google.com_0.localstorage	*	Internet History
Data	com.android.browser/app_geolocation/GeolocationPermissions.db	*	Internet History
Data	/data/com.google.android.gm/databases/<mail-name>.db	conversations & messages	Gmail
cache	*	*	Gmail 7

FOR585: Advanced Smartphone Forensics

It is rare to conduct a digital forensic investigation that does not include a smartphone or mobile device. Often, the smartphone may be the only source of digital evidence tracing an individual's movements and motives and may provide access to the who, what, when, where, why, and how behind a case. FOR585 teaches real-life, hands-on skills that enable digital forensic examiners, law enforcement officers, and information security professionals to handle investigations involving even the most complex smartphones available today.

FOR585: Advanced Smartphone Forensics focuses on smartphones as sources of evidence, providing the necessary skills to handle mobile devices in a forensically sound manner, understand the different technologies, discover malware, and analyze the results for use in digital investigations by diving deeper into the file systems of each smartphone. Students will be able to obtain actionable intelligence and recover and analyze data that commercial tools often miss for use in internal investigations, criminal and civil litigation, and security breach cases. FOR585 addresses today's smartphone technologies and threats by studying real-life investigative scenarios. Dont miss the NEW FOR585!

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