# MOBILE DEVICE FORENSICS

Device Forensics January 2020

# SIMPSON GARFINKEL

- Simson L. Garfinkel is an Associate Professor at the Naval Postgraduate School in Monterey, California.
- 2010 Identifies 5 problems with DF - many still relevant

# Problem 1 - Increased cost of extraction & analysis.

## Data: too much and too complex!

- Increased size of storage systems


- Cases now require analyzing multiple devices
  - *—2 desktops, 6 phones, 4 iPods, 2 digital cameras = 1 case*

- Non-removable flash
  - *—It's hard to physically get to the data*

- Proliferation of operating systems, file formats and connectors
  - *—XFAT, XFS, ZFS, YAFFS2, Symbian, Pre, iOS,*

## Consider FBI Regional Computer Forensic Laboratories growth:

- Service Requests: 5,057 (FY08) → 5,616 (FY09) (+11%)
- Terabytes Processed: 1,756 (FY08) → 2,334 (FY09) (+32%)

# Problem 2 — RAM and malware forensics is really hard.

## RAM Forensics—in its infancy

- RAM structures change frequently (no reason for consistency)
- RAM is constantly changing

## Malware is especially hard to analyze:

- Encryption; Conditional execution
- Proper behavior of most software is not specified

## Malware can hide in many places:

- On disk (in programs, data, or scratch space)
- BIOS & Firmware
- RAID controllers
- GPU
- Ethernet controller
- Motherboard, South Bridge, etc
- FPGAs

# Problem 3 — Mobile phones are really hard to examine.

Cell phones present special challenges

No standard connectors

- No standard way to copy data out
- Difficult to image & store cell phones without changing them.

How do we validate tools against thousands of phones?

- No standardized cables or extraction protocols

NIST's *Guidelines on Cell Phone Forensics* recommends:

- "searching Internet sites for developer, hacker, and security exploit information."

How do we forensically analyze 100,000 apps?

# Problem 4 — Encryption and Cloud Computing make it hard to get to the data

## Pervasive Encryption — Encryption is increasingly present

TrueCrypt

- BitLocker
- File Vault
- DRM Technology


## Cloud Computing — End-user systems won't have the data

Google Apps

- Microsoft Office 2010
- Apple Mobile Me




*—But they may have residual data!*

# Problem 5 — Time is of the essence.

Most tools were designed to perform a complete analysis

Find all the files

- Index all the terms
- Report on all the data
- Take as long as necessary!

Increasingly we are racing the clock:

- Police prioritize based on statute-of-limitations!
- Battlefield, Intelligence & Cyberspace operations require turnaround in days or hours.

NIST Special Publication 800-101
Revision 1

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-101
Revision 1 (Draft)

# Guidelines on Mobile Device Forensics (Draft)

## Recommendations of the National Institute of Standards and Technology

Rick Ayers
Sam Brothers
Wayne Jansen



Guidelines on Mobile Device Forensics
(Draft)

Recommendations of the National Institute of Standards and Technology

Rick Ayers
Sam Brothers
Wayne Jansen

SOFTWARE AND SYSTEMS

Software and Systems Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

September 2013

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Dr. Patrick D. Gallagher, Under Secretary for Standards and Technology and Director

# MOBILE DEVICE CHARACTERISTICS

- microprocessor, read only memory (ROM), random access memory (RAM), a radio module, a digital signal processor, a microphone and speaker, a variety of hardware keys and interfaces, and a liquid crystal display (LCD)
- OS of a mobile device may be stored in either NAND or NOR memory while code execution typically occurs in RAM

| | Feature Phone | Smartphone |
|---|---|---|
| **Processor** | Limited Speed (~52Mhz) | Superior Speed (~1GHz dual-core) |
| **Memory** | Limited Capacity (~5MB) | Superior Capacity (~128GB) |
| **Display** | Small Size Color, 4k – 260k (12-bit to 18-bit) | Large size Color, 16.7 million (~24-bit) |
| **Card Slots** | None | MiniSDXC |
| **Camera** | Still | Still, Panoramic, and Video (HD) |
| **Text Input** | Numeric Keypad | Touch Screen, Handwriting Recognition, Built-in QWERTY-style Keyboard |
| **Voice Input** | None | Voice Recognition (Dialing and Control) |
| **Cell Interface** | Voice and Limited Data | Voice and High Speed Data (4G LTE) |
| **Positioning** | None | GPS receiver |
| **Wireless** | IrDA, Bluetooth | Bluetooth, WiFi, and NFC |
| **Battery** | Fixed/Removable, Li-Ion Polymer | Fixed/Removable, Rechargeable Li-Ion Polymer |



# Hardware Characterisation

# DRAFT SP 800-101 Rev. 1, Guidelines on Mobile Device Forensics

| | Feature Phone | Smartphone |
|---|---|---|
| **OS** | Closed | Android, BlackBerry OS, iOS, Symbian, WebOS and Windows Phone |
| **PIM (Personal Information Management)** | Phonebook, Calendar and Reminder List | Enhanced Phonebook, Calendar and Reminder List |
| **Applications** | Minimal (e.g., games, notepad) | Applications (e.g., games, office productivity and social media) |
| **Call** | Voice | Voice, Video |
| **Messaging** | Text Messaging | Text, Enhanced Text, Full Multimedia Messaging |
| **Chat** | Instant Messaging | Enhanced Instant Messaging |
| **Email** | Via text messaging | Via POP or IMAP Server |
| **Web** | Via WAP Gateway | Direct HTTP |

Software Characterisation

DRAFT SP 800-101 Rev. 1,
Guidelines on Mobile Device Forensics

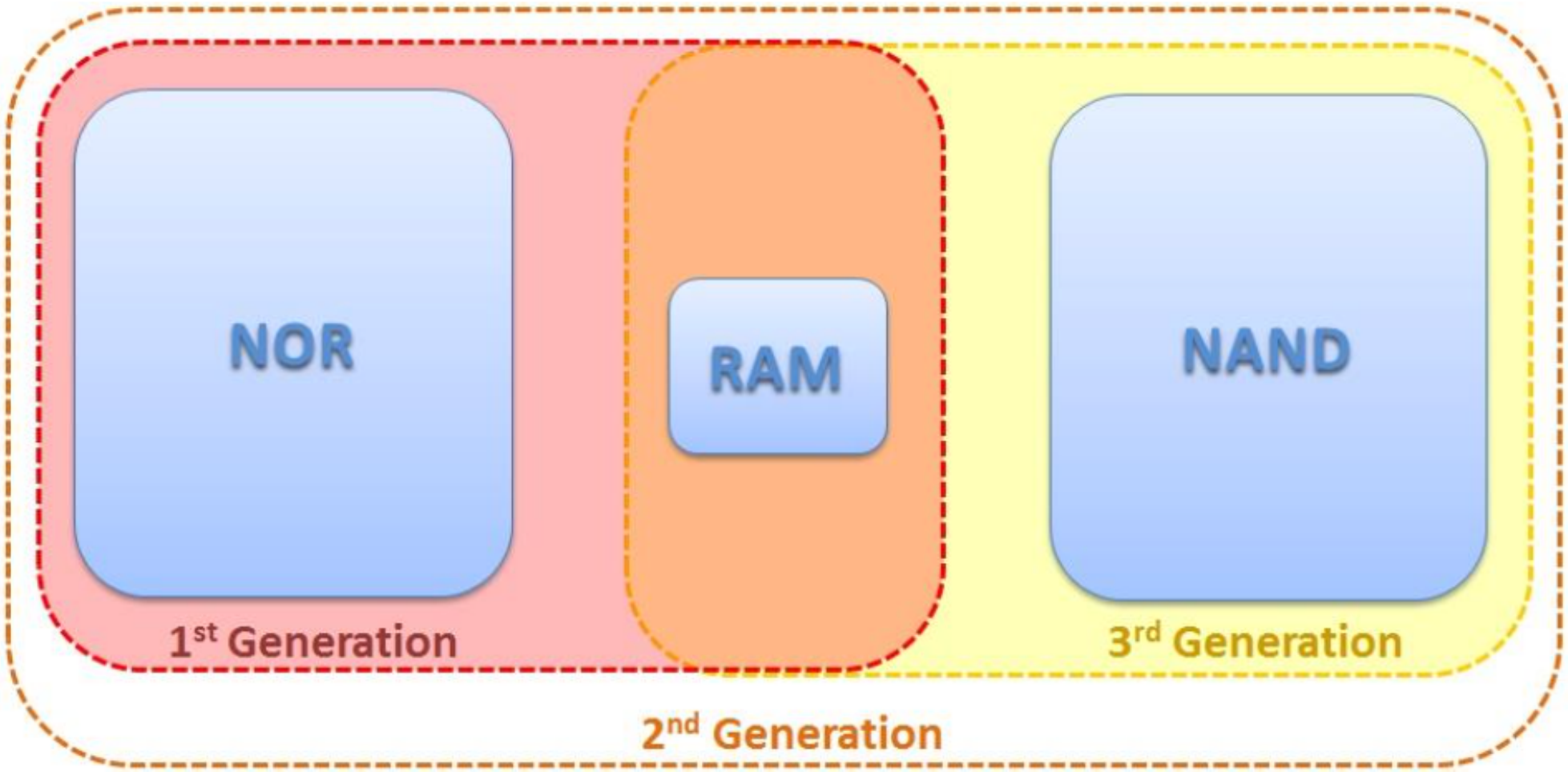
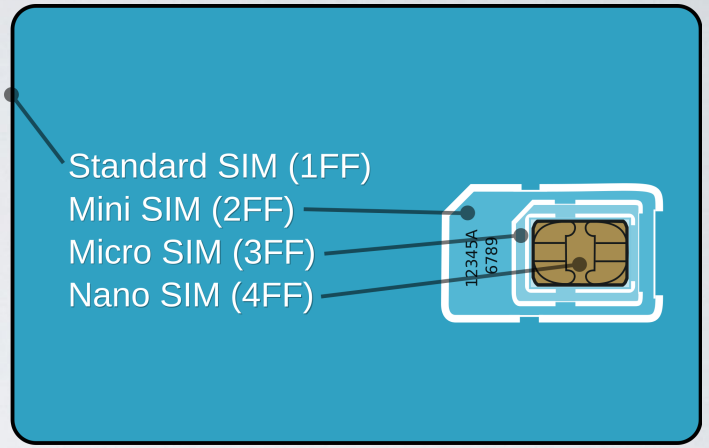



**Figure 1: Memory Configurations**


Mobile
Equipment
Universal
Integrated
Circuit Card
(UICC)

# UICC




Contains

a **processor** and between 16 to 128 KB of persistent electronically erasable programmable read only memory (**EEPROM**)

**RAM** for program execution

**ROM** for the operating system

user authentication and data encryption **algorithms**, and other applications

The UICC's file system resides in persistent memory and stores data such as:

phonebook entries

text messages

last numbers dialled (LND)

service-related information.

# OBSTRUCTED DEVICES

- hardware and software - flasher boxes
  - issues with rebooting, encryption, full memory, UI complexity and forensic use, documentation
- cold boot and smudge
- investigative methods
  - ask the suspect, review seized material, ask the service provider

https://www.youtube.com/watch?v=JDaicPIgn9U&feature=youtu.be

## ACPO Principle 1:

- No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

## ACPO Principle 2:

In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

## ACPO Principle 3:

An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

## ACPO Principle 4:

The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

# CRIME SCENE INVESTIGATION

# SEARCH TECHNIQUES

- Linkage, one piece leads to another
- Strip - walk in a line
- Spiral - move out from a point, evidence is though be close to this centre point
- Grid - Similar to a strip search but done in different directions
- Zone - for example different rooms
- Wheel or ray - used in special situations small circular crime scenes

# METHODOLOGY

- Do an initial walkthrough
- Look for 5w and h answers
- Once initial evaluation has occurred conduct a crime scene survey
- Note take, video, photograph & sketch

- Take notes as the search is done **NOTE TAKING**
- Consider the 5ws and h
- Include notification info (date, time, initial info received)
- Arrival information (method of transport, time, personnel present)
- Scene description
- Victim description
- Crime scene team and roles

# VIDEOGRAPHY

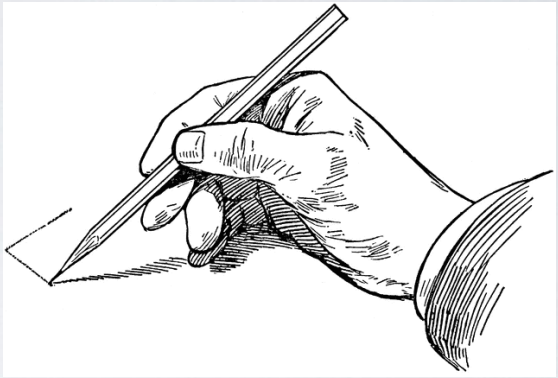
- Document the recording using a placard
- Do not include audio or members of the crime scene team
- Begin with the scene surroundings, e.g. entrances exits
- Record the victims' viewpoints, eg seat at desk
- Use a tripod and smooth movements
- Review at scene and re-record if needed. It is evidence and should not be edited afterwards. Copies can be made

# PHOTOGRAPHY

- Overall photos
- Mid-range photos
- Close-up photos


- Camera (SLR), 35, 50-60 and 28-35 mm lenses flash, tripod, image card, labelling materials, rulers, flashlight, extra batteries, photo log sheets

- Provides units of measurement for the crime scene
- Rough sketch & Finished sketch
- Over head view and side elevation
- 3D sketches not as common



- Triangulation, base line and polar coordinates are used for obtaining measurements
- Documentation includes title, caption, legends, abbreviations, scales

**SKETCHING**

# Records to be kept to comply with principle 3, ACPO

- Sketch map/photographs of scene and digital equipment;
- Record location and contact details;
- If a business, record opening hours;
- Details of all persons present where digital equipment is located;
- Details of digital items - make, model, serial number;
- Details of connected peripherals;
- Remarks/comments/information offered by user(s) of equipment;
- Actions taken at scene showing exact time;
- Notes/photographs showing state of system when found.

## To assist in the examination of the equipment, seize:

- Manuals of computer and software.

- Anything that may contain a password - PIN PUK etc.

- Encryption keys.

- Security keys – required to physically open computer equipment and media storage boxes eg: Apple sim pin key.

# Mobile Devices

- 1. Secure and take control of the area containing the equipment. Do not allow others to interact with the equipment;
- 2. Photograph the device in situ, or note where it was found, and record the status of the device and any on-screen information;
- 3. It is important to isolate the device from receiving signals from a network to avoid changes being made to the data it contains. For example, it is possible to wipe certain devices remotely and powering the device off will prevent this.

- 4. Seize cables, chargers, packaging, manuals, phone bills etc. as these may assist the enquiry and minimise the delays in any examination;
- 5. Packaging materials and associated paperwork may be a good source of PIN/PUK details;
- 6. Be aware that some mobile phone handsets may have automatic housekeeping functions, which clear data after a number of days. For example, some Symbian phones start clearing call/event logs after 30 days, or any other user defined period. Submit items for examination as soon as possible.

# ISOLATING DEVICES

- airplane mode
- wireless
- faraday box

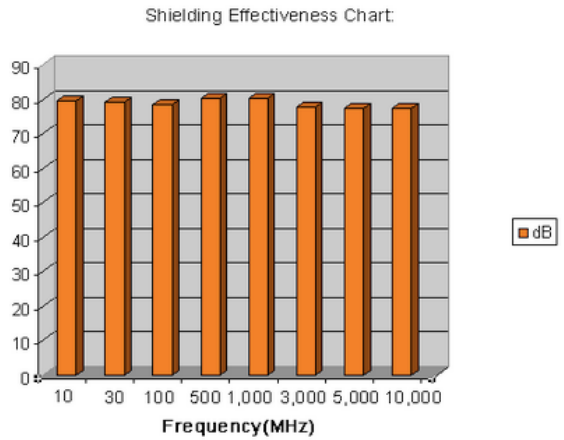
Paraben's StrongHold

Paraben's Tabletop StrongHold Tent was designed as a less expensive alternative to heavy, clunky RF shielding test enclosures. Protect your wireless evidence by placing it in the Tabletop StrongHold Tent while you perform your examination. The flexible gloves allow for smart phone screen manipulation while providing enough dexterity for you to type, remove cell phone batteries, or perform other necessary operations. You also have full range of motion allowing you to reach all areas of the enclosure without limitation. The Tabletop StrongHold Tent includes an LED light and a mesh viewing area that allows you to see inside the tent.

- Dimensions: 20" x 14" x 14"
- Double layered for extra protection
- Made in the USA
- Collapsible and portable

| Option | Pricing | Purchase |
|---|---|---|
| Tabletop StrongHold | $795.00 | + Add |
| Tabletop StrongHold with Project-A-Phone ICD-8000 | $1,295.00 | + Add |

- Brochure




example of a shielding device

The majority of the test cases proved that the shielding devices tested did not prevent network communication in all cases, and SMS messages most often penetrated the device while shielded, followed by voice calls and MMS messages. Three reasons why the shielding devices may fail are due to: the materials not providing enough attenuation, leaks or seams in the shield or the conductive shield acting as an antenna.

NIST Draft Guidelines on Mobile Device Forensics p32

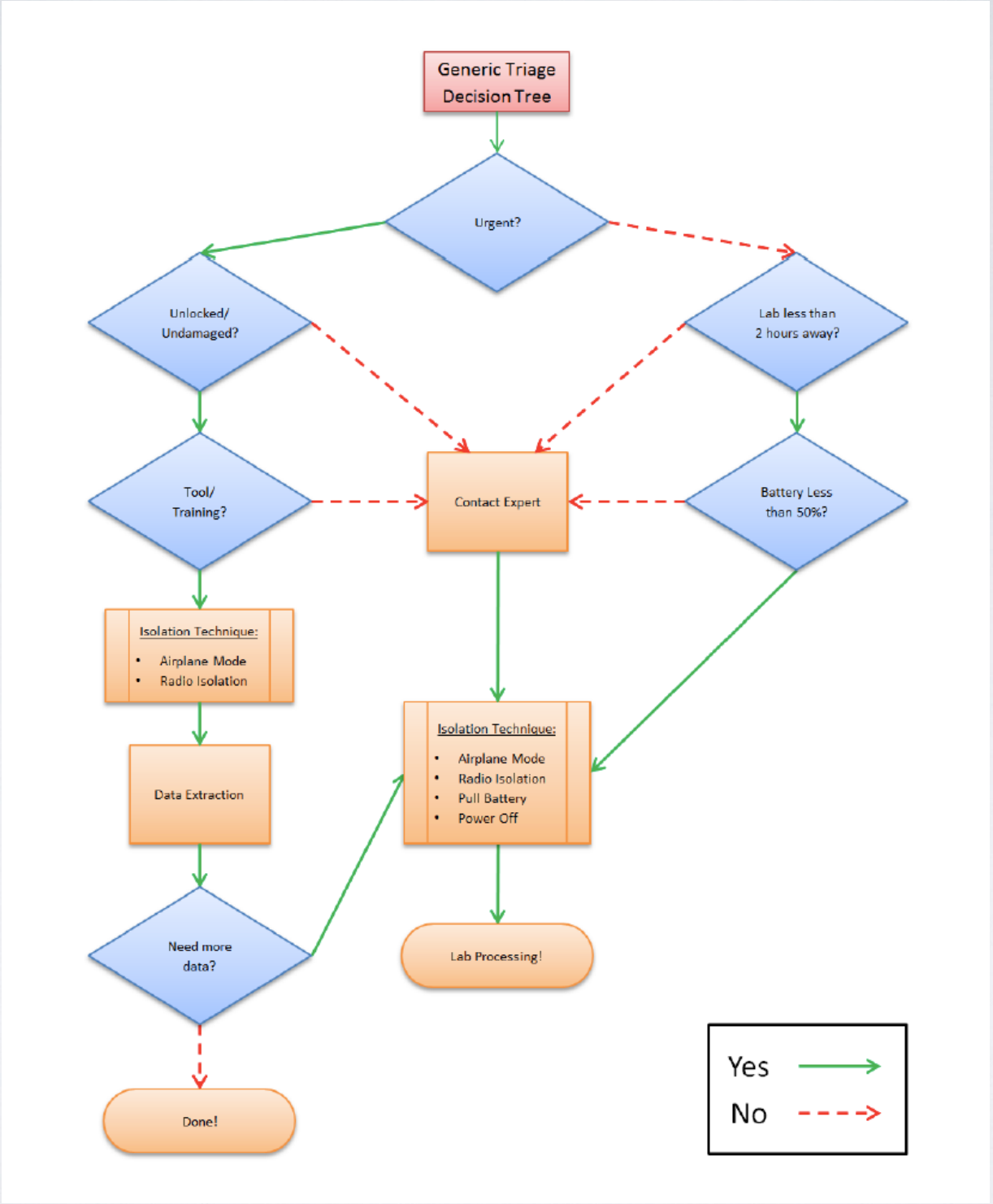
# CONSIDERATIONS

- security enhancements
- malicious software
- key remapping
- geo fencing
- explosives and booby traps

# ON-SITE TRIAGE

- Android and iOS devices, should be triage processed at the scene if they are found in an unlocked state, as the data may no longer be available to an investigator once the device's screen is locked, or if the battery exhausts
- Unlocked/Undamaged – Is the device in an unlocked state and functional permitting a manual or logical data extraction?
- Urgent – Do circumstances exist such that data extraction is required on site?
- Lab less than 2 hours away – Can the mobile device be transported to a forensics laboratory in less than 2 hours?
- Tool/Training – Is the device supported by the tool and has the examiner received proper training?
- Contact Expert – The on-site examiner should contact an expert for additional assistance and guidance.
- Battery Less than 50% – Does the device show that it has less than 50% remaining battery power?
- Need More Data - After the extraction is successful and the examiner has reviewed the results, is additional information or analysis required?

# Triage Decision Tree



# ON-SITE TRIAGE

- Android and iOS devices, should be triage processed at the scene if they are found in an unlocked state, as the data may no longer be available to an investigator once the device's screen is locked, or if the battery exhausts
- Unlocked/Undamaged – Is the device in an unlocked state and functional permitting a manual or logical data extraction?
- Urgent – Do circumstances exist such that data extraction is required on site?
- Lab less than 2 hours away – Can the mobile device be transported to a forensics laboratory in less than 2 hours?
- Tool/Training – Is the device supported by the tool and has the examiner received proper training?
- Contact Expert – The on-site examiner should contact an expert for additional assistance and guidance.
- Battery Less than 50% – Does the device show that it has less than 50% remaining battery power?
- Need More Data - After the extraction is successful and the examiner has reviewed the results, is additional information or analysis required?

# GATHERING EVIDENCE

- Once the mobile device is ready to be seized, the device should be **placed** in an appropriate container and labeled appropriately
- Due to **volatility** mobile devices should immediately be checked into a forensic laboratory for processing. The power requirements should be discussed with the evidence custodian. Battery powered devices held in storage for more than a day risk power depletion and data loss
- **Storage facilities** that hold evidence should provide a cool, dry environment appropriate for valuable electronic equipment. All evidence should be in sealed containers in a secure area with controlled access

# MOBILE DEVICE ACQUISITION

- Acquisition Levels
- Device Identification
- Device Acquisition
- Memory Cards
- Android Considerations

# LEVELS OF ACQUISITION

- 1. **Manual** – A process that involves the manual operation of the keypad and handset display to document data present in the phone's internal memory.
- 2. **Logical** – A process that extracts a portion of the file system.
- 3. **File System** - A process that provides access to the file system.
- 4. **Physical (Non-Invasive)** – A process that provides physical acquisition of a phone's data without requiring opening the case of the phone.
- 5. **Physical (Invasive)** – A process that provides physical acquisition of a phone's data requiring disassembly of the phone providing access to the circuit board. (e.g., JTAG)
- 6. **Chip-Off** – A process that involves the removal and reading of a memory chip to conduct analysis.
- 7. **MicroRead** – A process that involves the use of a high-power microscope to provide a physical view of memory cells.

# MOBILE DEVICE IDENTIFICATION

- device characteristics such as manufacturer logos, serial numbers, or design characteristics. Consult with online databases
- device interface, micro SD?
- carrier - device label in battery compartment if powered off. If powered on International Mobile Equipment Identifier (IEMI) can be found using *#06#

IMEI is a 15-digit number that indicates the manufacturer, model type, and country of approval for GSM devices. The initial 8-digit portion of the IMEI, known as the Type Allocation Code (TAC), gives the model and origin. The remainder of the IMEI is manufacturer specific, with a check digit at the end

# Features



Santoku includes a number of open source tools dedicated to helping you in every aspect of your mobile forensics, malware analysis, and security testing needs, including:

**Development Tools:**

- Android SDK Manager
- AXMLPrinter2
- Fastboot
- Heimdall (src | howto)
- Heimdall (GUI) (src | howto)
- SBF Flash

**Penetration Testing:**

- Burp Suite
- Ettercap
- Mercury
- nmap
- OWASP ZAP
- SSL Strip
- w3af (Console)
- w3af (GUI)
- Zenmap (As Root)

**Wireless Analyzers:**

- Chaosreader
- dnschef
- DSniff
- TCPDUMP
- Wireshark
- Wireshark (As Root)

**Device Forensics:**

- AFLogical Open Source Edition (src | howto)
- Android Brute Force Encryption (src | howto)
- ExifTool
- iPhone Backup Analyzer (GUI) (src | howto)
- libimobiledevice (src | howto)
- scalpel
- Sleuth Kit

**Reverse Engineering:**

- Androguard
- Antilvl
- APK Tool
- Baksmali
- Dex2Jar
- Jasmin
- JD-GUI
- Mercury
- Radare2
- Smali

# DEVICE ACQUISITION

- **Before** performing an acquisition, the version of the **tool** or device being used should be **documented**, along with any applicable patches or errata from the manufacturer applied to the tool
- Once the connection has been established, the forensic software suite or device may proceed to **acquire data** from the mobile device
- **Date** and **time** should be recorded for baseline purposes (should have already been done if the device was seized)

# MEMORY CARD ACQUISITION

- Mobile device forensic tools that acquire the contents of a resident memory card normally perform a logical acquisition
- If the device is found in an active state, the mobile device internal memory should be acquired before removing and performing a physical acquisition of the associated media (e.g., microSD Card)
- If the device is found in a power off state, a physical acquisition of the removable media should be performed before the internal handset memory of the mobile device is acquired

# ANDROID DEVICE CONSIDERATIONS

- lots of customisations for different brands
- lots more apps available as easier to enter an app into the play store, lots more rogue apps also!
- most date found in SQLite tables
- screens can have a 3x3 touch screen lock - susceptible to a smudge attack or by obtaining the gesture key file
- As best practice, the microSD card should be write-blocked and imaged using standard digital forensic techniques

# TANGENTIAL EQUIPMENT

- memory cards
- synchronised host computers - may or may not have occurred
- cloud based storage - may be issues based on location, politics, encryption etc

| Name | Characteristics |
|---|---|
| MMCmicro | Dime size (length-14 mm, width-12 mm, and thickness-1.1 mm)<br>10-pin connector and a 1 or 4-bit data bus<br>Requires a mechanical adapter to be used in a full size MMCplus slot |
| Secure Digital (SD) Card | Postage stamp size (length-32 mm, width-24 mm, and thickness-2.1mm)<br>9-pin connector, 1 or 4-bit data bus<br>Features a mechanical erasure-prevention switch |
| MiniSD Card | Thumbnail size (length-21.5 mm, width-20 mm, and thickness-1.4 mm)<br>9-pin connector, 1 or 4-bit data bus<br>Requires a mechanical adapter to be used in a full size SD slot |
| MicroSD (formerly Transflash) and microSDXC | Dime size (length-15 mm, width-11 mm, and thickness-1 mm)<br>6-pin connector, 1 or 4-bit data bus |
| Memory Stick Micro | Dime size (length-12.5 mm, width-15 mm, and thickness-1.2 mm)<br>11-pin connector, 4-bit data bus |


HOME

**GENERAL INFORMATION**

- CFTT Methodology Overview
- Presentations
- Contacts

**TECHNICAL INFORMATION**

- Disk Imaging
- Forensic Media Preparation
- Write block (Software)
- Write block (Hardware)

# Mobile Devices

**MOBILE DEVICES IMAGING SPECS**

- Mobile Device Tool Specification - (Version 2.0, March 2016)
- Mobile Device Tool Test Assertions and Test Plan - (Version 2.0, March 2016)
- Mobile Device Tool Specification (Version 1.0, July 8, 2014)
- Mobile Device Tool Test Assertions and Test Plan (Version 1.0, July 8, 2014)
- Smart Phone Tool Test Assertions and Test Plan
- Smart Phone Tool Specification
- GSM Mobile Device and Associated Media Tool Test Assertions and Test Plan
- GSM Mobile Device and Associated Media Tool Specification
- Non-GSM Mobile Device Tool Specification
- Non-GSM Mobile Device Tool Test Assertions and Test Plan

**TEST SUPPORT SOFTWARE**

- See Federated Testing

**TEST SET-UP DOCUMENTS**

- Mobile Device Data Population Setup Guide - (Version 1.0, March 2016)

- Deleted File Recovery
- Mobile Devices
- Forensic File Carving
- String Search

DHS Test Reports

NIJ's e-crime site published test reports (Before March 2013)

Computer Forensics Tool Catalog

Federated Testing

NSRL Website

CFReDS Project

Privacy Policy/Security Notice Disclaimer | FOIA

NIST is an agency of the U.S. Commerce Department


Date created: 8/20/2003
Last updated: October 5, 2016

Technical comments: cftt@nist.gov

**DHS REPORTS -- Test Results for Mobile Device Acquisition Tool**
(Find all DHS Reports here)

- Oxgen Forensics v8.3.1.105 (August 2016)
- Secure View v4.1.9 (July 2016)
- UFED Touch v4.4.0.1 [illegible] Internal Build 4.2.8.36 (July 2016)
- BlackLight v2016.1 (May 2016)
- Device Seizure v7.4 build 5921.15166 (May 2016)
- UFED 4PC v4.2.6.5 - Physical Analyzer (January 2016)
- MOBILedit Forensic v7.8.3.6085 (12/18/2015)
- Phone Forensics Express v2.1.2.2761 (12/18/2015)
- Device Seizure v6.8 (June 2015)
- Lantern v4.5.6 (June 2015)
- EnCase Smartphone Examiner v7.10.00.103 (April 2015)
- Oxygen Forensic Suite 2015 - Analyst v7.0.0.408 (March 2015)
- Secure View v3.16.4 (February 2015)
- viaExtract v2.5 (December 2014)
- Mobile Phone Examiner Plus v5.5.3.73 (December 2014)
- iOS Crime Lab v1.0.1 (December 2014)
- UFED Physical Analyzer v3.9.6.7 (October 2014)
- XRY/XACT v6.10.1 (September 2014)
- EnCase Smartphone Examiner v7.0. (April 2013)
- Device Seizure v5.0 build 4582.15907 (February 2013)
- Lantern v2.3 (February 2013)
- Micro Systemation XRY v6.3.1 (February 2013)
- Secure View 3v3.8.0 (February 2013)
- CelleBrite UFED 1.1.8.6 -- Report Manager 1.8.3/UFED Physical Analyzer 2.3.0 (October 2012)
- Mobile Phone Examiner Plus (MPE+) 4.6.0.2 (October 2012)
- AFLogical 1.4 (December 2011)
- Mobilyze 1.1 (January 2011)
- iXAM Version 1.5.6 (December 2010)
- Zdziarski's Method (December 2010)
- WinMoFo Version 2.2.38791 (November 2010)
- Secure View 2.1.0 (November 2010)
- Device Seizure 4.0 (November 2010)
- XRY 5.0.2 (November 2010)
- CelleBrite UFED 1.1.3.3 - Report Manager 1.6.5 (October 2010)
- BitPim - 1.0.6-official (January 2010)
- MOBILedit! Forensics 3.2.0.738 (January 2010)
- Susteen DataPilot Secure View 1.12.0 (September 2009)
- Final Data - Final Mobile Forensics 2.1.0.0313 (September 2009)
- Paraben Device Seizure 3.1 (September 2009)
- Cellebrite UFED 1.1.05 (September 2009)
- Micro Systemation .XRY 3.6 (October 2008)
- Guidance Software Neutrino 1.4.14 (October 2008)
- Paraben Device Seizure 2.1 (October 2008)
- Susteen DataPilot Secure View 1.8.0 (October 2008)

**NOTE:** Test reports are being updated to ensure 508 compliance. Currently some reports are unavailable. If you need one that is not linked above, please contact: cftt@nist.gov

- Mobile Devices
- Forensic File Carving
- String Search

**DHS Test Reports**

**NIJ's e-crime site published test reports (Before March 2013)**

**Computer Forensics Tool Catalog**

**Federated Testing**

**NSRL Website**

**CFReDS Project**

Privacy Policy/Security Notice
Disclaimer | FOIA

NIST is an agency of the U.S. Commerce Department


Date created: 8/20/2003
Last updated: 1/17/2018

Technical comments: cftt@nist.gov

## DHS REPORTS -- Test Results for Mobile Device Acquisition Tool

(Find all DHS Reports here)

- Test Results for Mobile Device Acquisition Tool - Blacklight v2016.3.1 (December 2017)
- Test Results for Mobile Device Acquisition Tool - Mobilyze v2017.1 Test Results (December 2017)
- Test Results for Mobile Device Acquisition Tool -UFED4PC v6.2.1/ Physical Analyzer v6.3.0.284 (September 2017)
- Test Results for Mobile Device Acquisition Tool - UFED4PC v6.2.1/ Physical Analyzer v6.3.0.284 (September 2017)
- Test Results for Mobile Device Acquisition Tool - XRY Kiosk v7.3.0 (August 2017)
- Test Results for Mobile Device Acquisition Tool - XRY v7.3.1 (August 2017)
- Test Results for Mobile Device Acquisition Tool - Lantern v4.6.8 (July 2017)
- Test Results for Mobile Device Acquisition Tool - Electronic Evidence Examiner Device Seizure v1.0.9466.18457 (April 2017)
- Test Results for Mobile Device Acquisition Tool - Mobile Phone Examiner Plus v5.6.0 (March 2017)
- Test Results for Mobile Device Acquisition Tool - MOBILedit Forensic Express v3.5.2.7047 (March 2017)
- Test Results for Mobile Device Acquisition Tool - XRY Kiosk v7.0.0.36568 (January 2017)
- Test Results for Mobile Device Acquisition Tool - MOBILedit Forensic v8.6.0.20354 (December 2016)
- Test Results for Mobile Device Acquisition Tool - MOBILedit Forensic v8.6.0.20354 (November 2016)
- Test Results for Mobile Device Acquisition Tool - XRY v7.0.1.37853 (November 2016)
- Test Results for Mobile Device Acquisition Tool - Oxygen Forensics v8.3.1.105 (August 2016)
- Test Results for Mobile Device Acquisition Tool - Secure View v4.1.9 (July 2016)
- Test Results for Mobile Device Acquisition Tool - UFED Touch v4.4.0.1 - Internal Build v4.2.8.36 (July 2016)
- Test Results for Mobile Device Acquisition Tool - Device Seizure v7.4 build 5921.15166 (May 2016)
- Test Results for Mobile Device Acquisition Tool - BlackLight v2016.1 (May 2016)
- Test Results for Mobile Device Acquisition Tool - UFED 4PC v4.2.6.5 - Physical Analyzer v4.2.6.4 (January 2016)
- Test Results for Mobile Device Acquisition Tool - MOBILedit Forensic v7.8.3.6085 (December 2015)
- Test Results for Mobile Device Acquisition Tool - Phone Forensics Express v2.1.2.2761 (December 2015)
- Test Results for Mobile Device Acquisition Tools - Device Seizure v6.8 (June 2015)
- Test Results for Mobile Device Acquisition Tools - Lantern v4.5.6 (June 2015)
- Test Results for Mobile Device Acquisition Tools - EnCase Smartphone Examiner v7.10.00.103 (April 2015)
- Test Results for Mobile Device Acquisition Tools - Oxygen Forensic Suite 2015 - Analyst

# POTENTIAL EVIDENCE

- Subscriber and equipment identifiers
- Date/time, language, and other settings
- Phonebook/Contact information
- Calendar information
- Text messages
- Outgoing, incoming, and missed call logs
- Electronic mail
- Photos
- Audio and video recordings
- Multi-media messages
- Instant messaging
- Web browsing activities
- Electronic documents
- Social media related data
- Application related data
- Location information
- Geolocation data

# TYPES OF INVESTIGATION

- an incident has occurred but the identity of the offender is unknown
- the suspect and the incident are both known

- objectives:
  - Gather information about the individual(s) involved {who}.
  - Determine the exact nature of the events that occurred {what}.
  - Construct a timeline of events {when}.
  - Uncover information that explains the motivation for the offence {why}.
  - Discover what tools or exploits were used {how}.

# TYPES OF ANALYSIS

Ownership and possession

Timeframe analysis

Data hiding analysis

Application and file analysis

# REPORT MAY INCLUDE (NIST)

- Identity of the **reporting agency**
- **Case identifier** or submission number
- Case **investigator**
- Identity and signature of the **examiner**
- Identity of the **submitter**
- **Date** of **receipt**
- Date of **report**
- Descriptive list of **items submitted** for examination, including serial number, make, and model
- The **equipment and set up used** in the examination
- Brief description of **steps taken** during examination, such as string searches, graphics image searches, and recovering erased files.
- Supporting materials such as printouts of particular items of evidence, digital copies of evidence, and chain of custody documentation
- Details of **findings**:

# Details of Findings

- **Specific files** related to the request
- **Other files**, including deleted files, that support the findings
- **String** searches, keyword searches, and text string searches
- **Internet**-related evidence, such as Web site traffic analysis, chat logs, cache files, e-mail, and news group activity
- Graphic **image** analysis
- Indicators of **ownership**, which could include program registration data
- **Data analysis**
- Description of relevant **programs** on the examined items
- **Techniques used to hide or mask data**, such as encryption, steganography, hidden attributes, hidden partitions and file name anomalies

# REPORT INFORMATION

(SWGDE BEST PRACTICES FOR MOBILE PHONE FORENSICS VERSION: 2.0 (FEBRUARY 11, 2013))

- **Evidence handling documentation should include but is not limited to:**
  - Copy of legal authority,
  - Chain of custody,
  - Detailed description and/or photographs of the phone (e.g., phone number, make, and model).
  - Photographs or documentation of any visible damage.
  - Information regarding the packaging and condition of the phone.
- **Examination documentation should be preserved according to policy and include:**
  - Sufficient detail to enable another examiner, competent in the same area of expertise, to repeat the findings independently.
  - Tools and software used in the examination.
  - Documentation of any anomalies in the data acquisition (e.g., acquisition disruptions, faulty cables, and incoming data).
  - Substantive communication notes regarding the case,
- **Report of findings:**
  - Seek to address **case specific requests** from the investigator.
  - Identify the **scope** and/or purpose of the examination.
  - Provide a detailed **description** of the mobile phone examined (e.g., phone number, carrier, owner, make/model, and OS).
  - Supplement reports related to the examination.
  - Include examiner name and date of exam.
  - Provide the relevant information in a clear and concise manner.