Mobile Device Evidence v.1.x

Map 1 → Mobile Device Evidence

- **Collection & Preservation**
  - Preparation
    - Check tools and equipment
    - Check/Ensure legal authority to collect evidence
  - Documentation
    - Non-electronic materials
      - Documents
      - Manuals
      - Cables
      - Packaging materials
      - Unlock Codes
    - Device
      - IMEI
      - IMSI
      - MEID
      - ESN
      - MAC address
    - Photographing
      - Scene
      - Evidence
      - Peripherals
      - Displays
- **Evidence Handling**
  - Evidence Preservation (1st Responder)
    - Device On?
      - YES
        - Can You Access System Settings

- YES
  - Network Isolation
    - Disconnect Device From Network
    - Enable Airplane Mode
    - Disable BT/Wifi
    - Put in RF shielded enclosure,
  - Turn On USB Debugging & Stay Awake (Android)
  - Extend Display Auto Lock/ Timeout & Lock Timer
  - Do Not Turn Off - Keep Charged
  - Collect Device Identifier
- NO
  - Do Not Turn Off - Keep Charged
  - Collect Device Identifier
  - Put In Faraday Bag

- NO
  - DO NOT TURN DEVICE ON
    - Was Device Discovered In Liquid
      - YES
        - Keep Device In Liquid Until Cleaned
        - Collect Device Identifier If Possible (ANDROID)
        - Remove Battery if Possible
      - NO
        - Remove Battery If possible
        - Collect Device Identifier

- Traditional Forensics
  - Secure Fingreprints
  - Secure DNA

Evidence Acquisition

- Evidence Acquisition
  - Device Identification

- Device Identification
  - FCC ID
  - IMEI
  - MEID
  - ESN
  - ESN
- Extraction Methods
  - Manual
    - Manual operation of keypad/handset
  - Logical
    - Extraction of files and objects
  - File System
    - Files, objects and data extracted with filesystem
  - Physical (Non-Invasive)
    - Forensic Acquisition by HW/SF tools
  - Physical (Invasive)
    - JTAG
    - ISP (In-System Programming)
    - Chip-Off
  - Removable Media
  - GSM Mobile Device Considerations
    - If devices requiring a UICC/SIM, process UICC/SIM first
- Access
  - Smart Locks?
    - On Body Detection
      - Owner
      - Trusted 3. party
    - Trusted Places
      - Home
      - Trusted Location/zone

- Trusted Devices
  - Trusted BT device (Watch)
- Device Powered On and Locked
  - Password Guessing Strategy?
- Device Powered On and Unlocked
  - Collected on-site as soon as possible.
  - Keep Awake / Charge
- Mobile Device Management (MDM)
  - Seek assistance from SysAdm
- Physical Encryption?
- Backup Encryption?

Mobile Operating Systems

- Android:
  - Vendors
    - Samsung
    - LG
    - Google
    - HTC
    - Sony
    - Motorola
    - Huawei
  - Google Account
    - Drive
    - Maps
    - Calendar
    - Additional Evidence Sources
  - Google Play
    - Review Installed Applications
  - XML Files
- iOS

- iCloud
  - iMessages
  - FaceTime
  - iCloud
  - Appstore
  - Findy My Device
  - Apple Music
- Apple Service
- iMessage
  - Devices synced by an AppleID
  - Can be routed as SMS/MMS
- FaceTime
  - FaceTime records may reside on device
- Apple Store
  - AppleID
  - Date/Time for purchase
  - Look for "sideloaded apps"
- iOS Time Format
  - UNIX Epoch
  - CF Absolute Time
- Plists
- Google Account
  - Drive
  - Maps
  - Calendar
  - Additional Evidence Sources

- Linux
  - Google Account
    - Drive
    - Maps

        - Calendar
        - Additional Evidence Sources
    - Windows Mobile
        - Google Account
            - Drive
            - Maps
            - Calendar
            - Additional Evidence Sources
        - Office365 Account
    - Other
        - Older legacy systems

- **Forensic Analysis**
    - Data/Objects Of Value
        - Subscriber / 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
        - Videos and included metadata such as XMP
        - 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

- Forensic Tool Analysis
  - Parse & Search Data
  - Identify & Tag Key Evidence
- Validation
  - Compare sample results against other tools
  - Manually examine data where it resides within the device extraction
  - Compare the parsed content with content that is actually viewable on the subject device
  - Properly address and document contradictions
- Evidentiary Considerations
  - Logical encryption
  - Data hiding applications
  - Timeline analysis
  - Malware Detection

- **Created by @tabalizer**
  The purpose of this map 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.