

iOS Forensics

(Part 1)



Contents

- Introduction
- Seizure and Isolation
- Types of Acquisition
- Operating modes of iOS devices
- Jailbreaking
- Summary



Introduction

- Mobile forensics is a branch of digital forensics related to the recovery of digital evidence from mobile devices
- “Forensically sound” is a term used extensively in the digital forensics world to qualify and justify the use of a particular forensic technology or methodology
- The central principle for a sound forensic examination is that the original evidence must not be modified



Seizure and Isolation

- Note location from where mobile has been collected.
- Take the picture using camera and take picture of the location
- **Chain of Custody**
 - Is a document to maintain each record of the Digital evidence from the collection to presentation
 - Another part of documentation is taking pictures (photographs) of the crime scene, capturing the original state of the mobile device, as well as the make, model, serial number, IMEI number or operating system version .which would help during the acquisition phase and need to be captured as well
- Take the picture of the mobile phone before starting any progress
- Request for Passcode, SIM pin, iTunes backup password if possible
- Check for any Unified Endpoint Management solutions
- Note the status of the device
 - Whether it's powered off or on
 - If it is power on then, check the battery status, network status
 - Check where the screen is locked
- Search/request for the SIM and if any cables are located around



Seizure and isolation (Cont'd)

Four (4) Major points

- Circumventing the passcode/iTunes backup password is not always possible
 1. Try to secure the passcode from the owner and/or immediately disable the passcode requirement if the phone is accessible
 2. Place the phone in “airplane mode”
 3. Change the setting, the Auto-lock feature to “never” would be a desired setting for the duration of forensic acquisition
 4. Document the settings changed prior to taking a forensic image



Seizure and isolation(Cont'd)

Isolation Techniques (If iOS device turned ON)

- Place the phone in “airplane mode”
- Check and manually disable, if necessary, "hotspots" or any GPS locations, the Wi-Fi and Bluetooth toggles mode (these may be left on even in Airplane mode if the user enabled Wi-Fi once in that mode)
- Connect the phone to a power bank
- Do not remove the SIM card at this point. There maybe scenarios where it is found that devices lock up when the SIM card is removed
- Use a Lightning adapter to prevent USB Restricted mode from being activated (for devices running iOS 11.4.1 only; iOS 12 and 13 may restrict USB immediately)
- If you have a Faraday bag handy, place the phone along with the adapter and charger into the Faraday bag

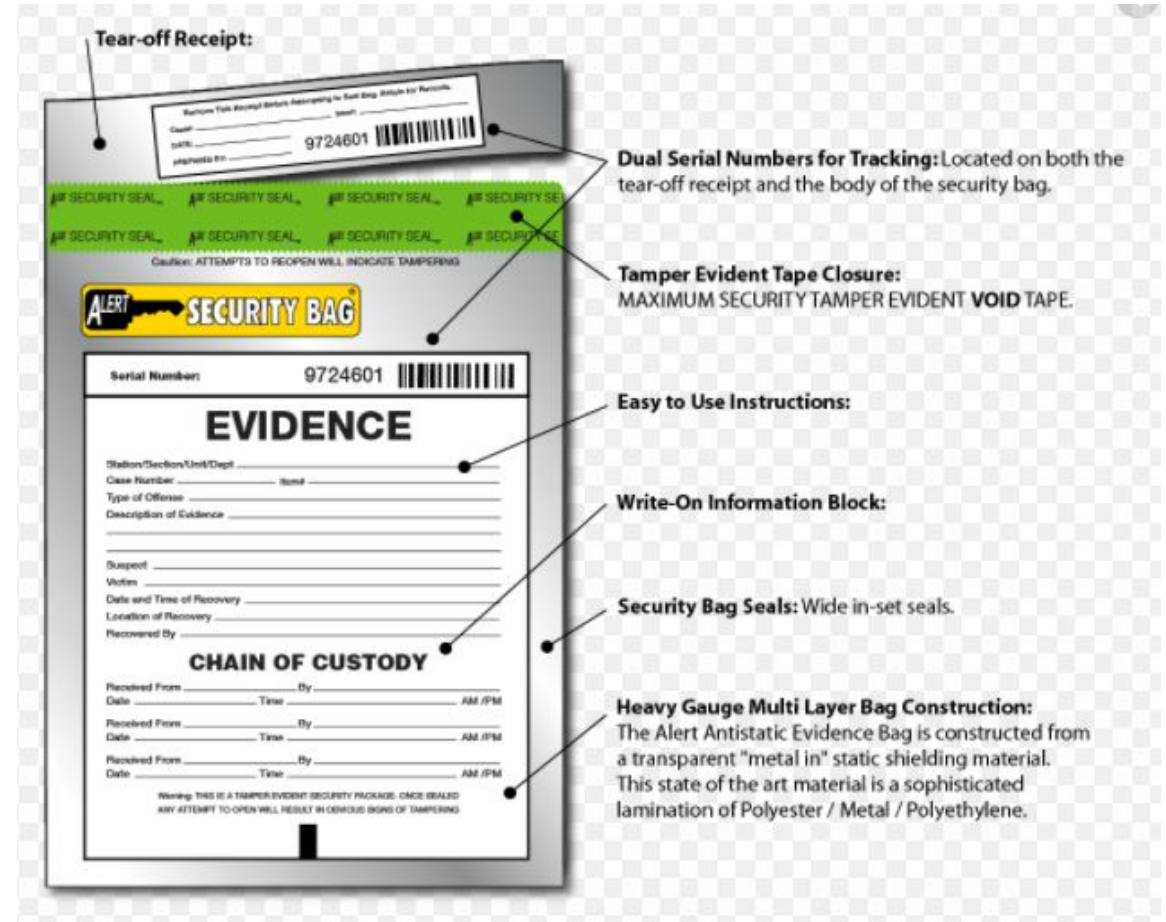
Faraday bag



Seizure and Isolation (Cont'd)

Isolation Techniques (If device is OFF, DO NOT turn ON.)

- Place it in an Evidence Bag or Box
- If you have a Faraday bag handy, place the phone along with the adapter and charger into the Faraday bag
- Bring it back to Forensic Lab
- Back in the Forensic Lab
- You will want to remove the SIM card
- Do a proper acquisition of the SIM
- You will have to turn on the phone if necessary, and treat it as if it was turn on and apply the Isolation Techniques



Seizure and Isolation (Cont'd)



Forensic acquisition

- is the process of acquiring the original evidence in a forensically sound manner while maintaining the integrity of it
- This process is also known as “Imaging”
- It can be done on site (at the scene) and can also be done off-site (in the lab)

Hashing

- Done after acquisition of device
- Hashing is the method used to prove the integrity of the evidence
- MD5 or SHA are widely used algorithms to calculate the Hash values
- Hash values should be documented as well to maintain record of the Digital evidence.

Types of Acquisition



Logical

SMS

Contact

Call Logs

Media

App Data

File System

SMS

Contact

Call Logs

Media

App Data

Files

Hidden Files

Physical

SMS

Contact

Call Logs

Media

App Data

Files

Hidden Files

Deleted Data

Types of Acquisition(Cont'd)



Advance Logical

- Combines both Logical and File System extraction methods

Cloud acquisition

- iCloud backups
- iCloud Drive (full content, including third-party app data not available by any other means)
- iCloud Photos
- FileVault2 recovery token (FileVault is a disk encryption program in Mac Operating system)
- iCloud keychain
- Health data
- Messages (iMessage and SMS)

Types of Acquisition(Cont'd)

Draw backs on cloud acquisition

- Need proper authentication credentials
- Need the user's Apple ID and password, plus the second, two factor - authentication factor (if 2FA is enabled)



Types of Acquisition(Cont'd)



Acquisition via iTunes Backup

- If iOS device not available. A backup would be retrieved from the workstation (Windows or MacOS)
- Device typically connects to for updates or syncing music, movies and applications
- It should be noted that iTunes performs an automated backup during the sync process and/or when an upgrade to the iOS is performed
- Backups are stored in alternate locations depending on the OS

Operating Systems	File Location
Windows XP	%systempartition%\documents and settings\%username%\Application Data\Apple Computer\MobileSync\Backup
Windows Vista 7, 8 or 10	%systempartition%\Users\%username%\AppData\Roaming\Apple Computer\MobileSync\Backup\
MacOS	Users/%username%/Library/Application Support/MobileSync/Backup

Types of Acquisition(Cont'd)

Manual

- The examiner uses the user interface of the phone to browse and investigate
- No special tools or techniques are required
- Manual Extraction of Chat messages (Screen Shots, export to external media)
- limitation is that only the files and data visible through the normal user interface
- Data extracted through other methods can also be verified using this.
- Very easily modify data on the device

Brute Force

- offensive techniques like passcode cracking, Jail Breaking



Operating modes of iOS devices

- IOS devices can be operated in three modes.
 - Normal mode
 - Recovery mode
 - DFU mode
- It is necessary that examiner or Investigator should be aware of this mode as this knowledge is required to decide during the forensic acquisition that on which mode device should be operated to allow efficient extraction of data.



Operating modes of iOS devices

Normal Mode

- When iPhone is switched on, it boots in an operating system
- In normal mode, the user could perform all regular activities
- Normal mode boot process consists of three (3) steps:
 - Low-Level Bootloader
 - iBook
 - iOS kernel
- These boot steps are signed to keep the integrity of the process



Operating modes of iOS devices (Cont'd)

Recovery Mode

- The device enters into recovery mode
- if during the normal boot process if any step is failed to load or verify



Operating modes of iOS devices (Cont'd)

DFU mode (Device Firmware Upgrade)

- Used to perform IOS upgrading, and it is a low-level mode for diagnosis
- During boot up, if Boot ROM is not getting a load or verify, then iPhone presents the Black screen



Jailbreaking

- Jailbreaking is the process of exploiting the flaws of a locked-down electronic device to install software other than what the manufacturer has made available for that device
- Jailbreaking allows the device owner to gain full access to the root of the operating system and access all the features
- user could gain access to all partitions including file system with read-write only permissions
- This method is not accepted forensically because it may overwrite some important data but it allows performing physical acquisition efficiently
- This method is used when root access of the file system is required as well as for the physical acquisition



Jailbreaking

Implications

- Apple considers jailbreaking iOS to be a violation of its terms and conditions of use and advises customers that the practice exposes a phone to several risks, including:
 - Security vulnerabilities
 - Stability issues
 - Potential crashes and freezes
 - Shortened battery life



Summary

- We understand the importance process of mobile forensic
- It is necessary that examiner or Investigator should be aware of the types of acquisition and Operating modes of i O S devices. This knowledge is required to decide during the forensic acquisition, that which mode device should be operated to extract data
- Lastly what is Jailbreaking. How it can help in forensic acquisition. however there will be implications.
- Such as violation of its terms and conditions of use.
- Exposes a phone to several risks, including: Security vulnerabilities, Stability issues, Potential crashes and freezes, Shortened battery life.

