1. Introduction to Mobile Forensics

Mobile cellular subscription growth from 2005 to 2013

Mobile phone evidence extraction process
Cellular phone tool leveling pyramid (Sam Brothers, 2009)
2. Understanding the Internals of iOS Devices

Source: https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=9&qpcustomb=1

The iPhone model number located on the back of the case

The iPhone About screen, displaying firmware Version 5.1.1 (9B206)
The iPhone 5S teardown image—side one (included with kind permission from TechInsights)

The iPhone 5S teardown image—side two (included with kind permission from TechInsights)
The iPad 3 cellular model teardown image—side one (included with kind permission from Chipworks)

Included with kind permission from Chipworks
### The OS compatibility matrix

<table>
<thead>
<tr>
<th></th>
<th>iPhone OS 1.0</th>
<th>iPhone SDK 2.0</th>
<th>iPhone SDK 3.0</th>
<th>iPhone SDK 4.0</th>
<th>iOS 5</th>
<th>iOS 6</th>
<th>iOS 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPhone</td>
<td>1.0</td>
<td>3.1.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iPod Touch</td>
<td>1.1</td>
<td>3.1.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iPhone 3G</td>
<td>2.0</td>
<td>4.2.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iPod Touch (2nd Gen)</td>
<td>2.1.1</td>
<td>4.2.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iPhone 3GS</td>
<td>3.0</td>
<td></td>
<td>6.1.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iPod Touch (3rd Gen)</td>
<td>3.1.1</td>
<td></td>
<td>5.1.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iPad (1st Gen)</td>
<td>3.2</td>
<td>4.3.5</td>
<td>5.1.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iPhone 4</td>
<td></td>
<td>4.0 (GSM)/4.2.6 (CDMA)</td>
<td>7.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iPod Touch (4th Gen)</td>
<td></td>
<td>4.2.1</td>
<td></td>
<td>6.1.3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iPad2</td>
<td></td>
<td>4.3.5</td>
<td></td>
<td>7.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iPhone 4S</td>
<td></td>
<td></td>
<td>5.0</td>
<td>7.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iPad</td>
<td></td>
<td></td>
<td>5.1</td>
<td>7.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iPod Touch (5th Gen)</td>
<td></td>
<td></td>
<td></td>
<td>6.0</td>
<td>7.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>iPad Mini</td>
<td></td>
<td></td>
<td>6.0</td>
<td>7.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iPhone 5</td>
<td></td>
<td></td>
<td></td>
<td>6.0</td>
<td>7.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>iPhone 5C</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>7.0.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>iPhone 5S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>7.0.1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The iOS layers

The iOS security architecture
3. Data Acquisition from iOS Devices

A secure boot chain of an iPhone in normal mode
The redsn0w recovery fix

A secure boot chain of an iPhone in DFU mode
The MAC system information displaying a DFU-mode device

An exploited boot chain of an iPhone in DFU mode
The redsn0w welcome screen

The encrypted AddressBook file

The decrypted AddressBook file
4. Data Acquisition from iOS Backups

iTunes—disabling automatic sync

iTunes—iPhone locked message
iTunes—iPhone summary

Pairing records on the iPhone

Pairing record on a computer
iPhone backup files

System domains on the iPhone

iPhone Backup Extractor—choosing backups
Extracted iPhone backup files

<table>
<thead>
<tr>
<th>Service</th>
<th>Domain</th>
<th>Account</th>
<th>Date</th>
<th>Access group</th>
<th>Protection class</th>
</tr>
</thead>
<tbody>
<tr>
<td>apple.com</td>
<td></td>
<td>delight</td>
<td>2014-01-02</td>
<td>guest</td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>AirPort</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>iDevice Mobile Device ID</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>com.apple.certificates &amp; keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>com.apple.b8c1f6e0a6b-9a75bfa1-1f7aace4c0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>com.apple.certificates &amp; keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>com.apple.b8c1f6e0a6b-9a75bfa1-1f7aace4c0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>com.apple.certificates &amp; keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>com.apple.certificates &amp; keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>com.apple.certificates &amp; keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>com.apple.certificates &amp; keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>com.apple.certificates &amp; keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>com.apple.certificates &amp; keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>com.apple.certificates &amp; keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>com.apple.certificates &amp; keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>com.apple.certificates &amp; keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>com.apple.certificates &amp; keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>com.apple.certificates &amp; keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>com.apple.certificates &amp; keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>com.apple.certificates &amp; keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>com.apple.certificates &amp; keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>com.apple.certificates &amp; keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>com.apple.certificates &amp; keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>com.apple.certificates &amp; keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>com.apple.certificates &amp; keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>com.apple.certificates &amp; keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>com.apple.certificates &amp; keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>com.apple.certificates &amp; keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>com.apple.certificates &amp; keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>com.apple.certificates &amp; keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>com.apple.certificates &amp; keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
<tr>
<td>com.apple.certificates &amp; keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AlwaysFullyDeviceLocked</td>
</tr>
</tbody>
</table>

A decrypted keychain
iTunes—encrypted backup

iPhone Password Breaker—Choose backup

iPhone Password Breaker—password brute force
iCloud backup toggle on the iPhone
5. iOS Data Analysis and Recovery

The SMS Spotlight cache file

```
mbp-hmahaliks:Webkit hmahaliks cd /Users/hmahaliks/Desktop/WebKit/LocalStorage
```

TheLocalStorage folder contents

```
Table
Field | Columns | Size | Data
-----|---------|------|------
Columns Calibration | 0-80000000 | 9 | 1
Tables | 0-300000000 | 11 | 1
Fields | 0-1000000000 | 19 | 1
```

The Consolidated.db view with SQLite Professional

Keyboard cache in hex editor
6. iOS Forensic Tools

The Elcomsoft iOS Forensic Toolkit welcome screen

The Elcomsoft iOS Forensic Toolkit welcome screen

The Elcomsoft iOS Forensic Toolkit welcome screen

The EIFT passcode recovery options
EIFT supported devices

<table>
<thead>
<tr>
<th>Device Description</th>
<th>Physical Imaging</th>
<th>Logical Imaging</th>
<th>Passcode Recovery</th>
<th>Keychain Decryption</th>
<th>Disk Decryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPhone 3G iPod Touch 1 iPod Touch 2</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>not encrypted 2)</td>
</tr>
<tr>
<td>iOS 4</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>not encrypted 2)</td>
</tr>
<tr>
<td>iPhone 3GS iPod Touch 3 iPad 1</td>
<td>++</td>
<td>+</td>
<td>instant 2)</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>iOS 4/5</td>
<td>++</td>
<td>+</td>
<td>instant 2)</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>iPhone 4 iPod Touch 4</td>
<td>++</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>iOS 4/5/6/7</td>
<td>++</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>iPhone 4S iPhone 5 iPhone 5C iPad 2-4 iPad Mini iPod Touch 5</td>
<td>++</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>

Oxygen Forensic Suite—the Connection Mode screen
Oxygen Forensic Suite—the device information screen

Oxygen Forensic® Extractor
Select sections to be extracted from the device

- Apple iPhone 5s
- Contacts
- Call Log
- Event Log
- File structure
  - Selective reading
    - Images
    - Audio
    - Videos
    - Documents
    - Applications
    - Database files
    - Other files
  - Full reading
    - Files from internal memory
- Messages
- Phonebook
Oxygen Forensic Suite—the extracted data summary screen
UFED Physical Analyzer—the iOS Device Data Extraction Wizard screen

UFED Physical Analyzer—the device information screen
iRecovery Stick—the Choose connected device screen
7. Understanding Android

Android architecture

JVM versus DVM
The permission model in Android
8. Android Forensic Setup and Pre Data Extraction Techniques

Android SDK Tools setup wizard

Android SDK License
Android Virtual Device Manager

Virtual device configuration
The Android emulator

USB mass storage
HTC mobile USB options

The USB debugging option in Samsung mobiles
Smudges visible on a device under proper lighting (source: https://viaforensics.com/wpinstall/wp-content/uploads/smudge.png)

Forgot pattern option on an Android device

Normal Android system recovery mode
Modified recovery mode

Application requesting root access
9. Android Data Extraction Techniques

The `/data` directory extracted to a forensic workstation

SQLite Browser

The `contacts2.db` file copied to a local folder
Calls table in the contacts2.db file

The browser2.db file in Oxygen Forensic SQLite Viewer

The fb.db file in SQLite browser
The AFLogical OSE app

Data extraction completed.

Message displayed after the extraction is complete
Files extracted using ALogical OSE

The JTAG setup
The chip-off technique

WinHex view of Edit Mode (left) and WinHex Read-only Mode enabled (right)
The WinHex disk image option
10. Android Data Recovery Techniques

Android recovery—device detection

The list of storage devices available

 Recovered files list
The Super Backup Android app

Recovering deleted SMS messages
The scalpel configuration file

Running the Scalpel tool on a dd file

Output folder after running the Scalpel tool
Recovered data using the Scalpel tool

The Contacts menu in Gmail

The Restore Contacts dialog box
11. Android App Analysis and Overview of Forensic Tools

Facebook App in Google Play Store

Extracted files of an APK file

The classes-dex2jar.jar file created by the dex2jar tool
The JD-GUI tool

AFLogical in Santoku Linux

The AFLogical results
The UFED Touch main menu

The UFED touch—vendor list screen

The UFED Physical Analyzer application
The MOBILedit connection wizard

Navigation  Samsung Galaxy S III (Read-Only)

The MOBILedit connection wizard
The MOBILedit tool—Call logs option

The Autopsy tool screen

Autopsy image loading
Autopsy ingest modules

Autopsy results
Windows Phone Forensics

The Windows Phone home screen

Windows app requesting user permissions
The ChevronWP7 tool

Windows Phone Device Manager

<table>
<thead>
<tr>
<th>Name</th>
<th>Publisher</th>
<th>Installed On</th>
<th>Size</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>TouchWeather</td>
<td>Julien Schapman</td>
<td>28/02/2011</td>
<td>664.91 KB</td>
<td>1.0.0</td>
</tr>
<tr>
<td>TouchWeather</td>
<td>Julien Schapman</td>
<td>28/02/2011</td>
<td>2.42 MB</td>
<td>1.0.2</td>
</tr>
<tr>
<td>Bluetooth</td>
<td>Julien Schapman</td>
<td>28/02/2011</td>
<td>587.02 KB</td>
<td>1.0.0</td>
</tr>
<tr>
<td>Config advanced</td>
<td>Julien Schapman</td>
<td>28/02/2011</td>
<td>1.31 MB</td>
<td>1.1.0</td>
</tr>
<tr>
<td>Etoile de registre</td>
<td>Julien Schapman</td>
<td>28/02/2011</td>
<td>1.29 MB</td>
<td>1.1.0</td>
</tr>
<tr>
<td>Config Connection</td>
<td>HTC Corporation</td>
<td></td>
<td>513.10 KB</td>
<td>1.0.0</td>
</tr>
<tr>
<td>Convertisseur</td>
<td>HTC Corporation</td>
<td></td>
<td>1.82 MB</td>
<td>1.0.0</td>
</tr>
<tr>
<td>HTC Hub</td>
<td>HTC Corporation</td>
<td></td>
<td>18.04 MB</td>
<td>1.0.0</td>
</tr>
</tbody>
</table>

Windows Phone Device Manager—The Manage Applications screen
The store.vol file in Windows Phone

Windows Phone: extracting e-mail

Windows Phone: folder 3
Windows Phone: renaming data files to JPG files

Contents of the IsolatedStore folder

The DataCache.UserID folder of the Facebook app
13. BlackBerry Forensics

The BlackBerry Z10 support in Cellebrite UFED Touch

The BlackBerry Curve support in Cellebrite UFED Touch

The encrypted backup file password prompt
The encrypted backup file password prompt in Oxygen Forensics Suite

BlackBerry Desktop Manager
Full backup option in BlackBerry

Cellebrite Physical Analyzer—Address Book examination
Elcomsoft Phone Password Breaker

The Elcomsoft Phone Password Breaker attack options

Elcomsoft Phone Password Breaker
Telephone numbers parsed by Bulk Extractor

BlackBerry Backup Extractor

E-mail extracted from backup
Contacts extracted from backup

Other useful data extracted from the backup

The Hex view of IPD file

Oxygen Forensics Suite BlackBerry IPD Viewer
Oxygen Forensics Suite BlackBerry IPD Viewer—the encrypted file

The Oxygen Forensics Suite BlackBerry IPD Viewer results