

iOS Forensics

(Part 2)



Contents

- Introduction
- iOS Device
- iOS Architecture
- App Interaction with iOS
- iOS Standard Directories: Where Files Reside
- iOS File System
- Partitions
- Property List (Plist)
- SQL Lite Databases
- Exif Metadata
- Data Structure and Artifacts



Introduction

- iOS (formerly iPhone OS) is a mobile operating system created and developed by Apple Inc.
- Apple developed an operating system for iPhone, iPad and iPod Touch
- Devices running on iOS operating system are called iOS devices
- iOS devices provide larger storage space which could store Emails, Browsing histories, chat histories, Wi-Fi data and GPS data
- From the forensics perspective, such devices could present lots of useful artifacts during the investigation



iOS Devices

iPhone

- Most popular among IOS devices is iPhone, due to design, Camera and Features

iPad

- After the Huge success of the iPhone
- Apple launched iPad tablet known as iPad or iPad first Generation. It was released after the iPhone 3Gs

iPod

- First iPod was launched by Apple in 2001. It was known as “First Generation”
- Subsequent have been referred as “Second Generation” so on
- Initial lunched as Music play but it advances to have the ability to play Videos and Games to users
- An examiner could retrieve forensic data from storage, browser, gallery, etc. on an iPod
- iPod Touch models featured
 - Camera, Wi-Fi Capabilities, Safari web browser, Storage and Playback for Audio, Video and Photo, YouTube player
 - Apps could be installed from App store

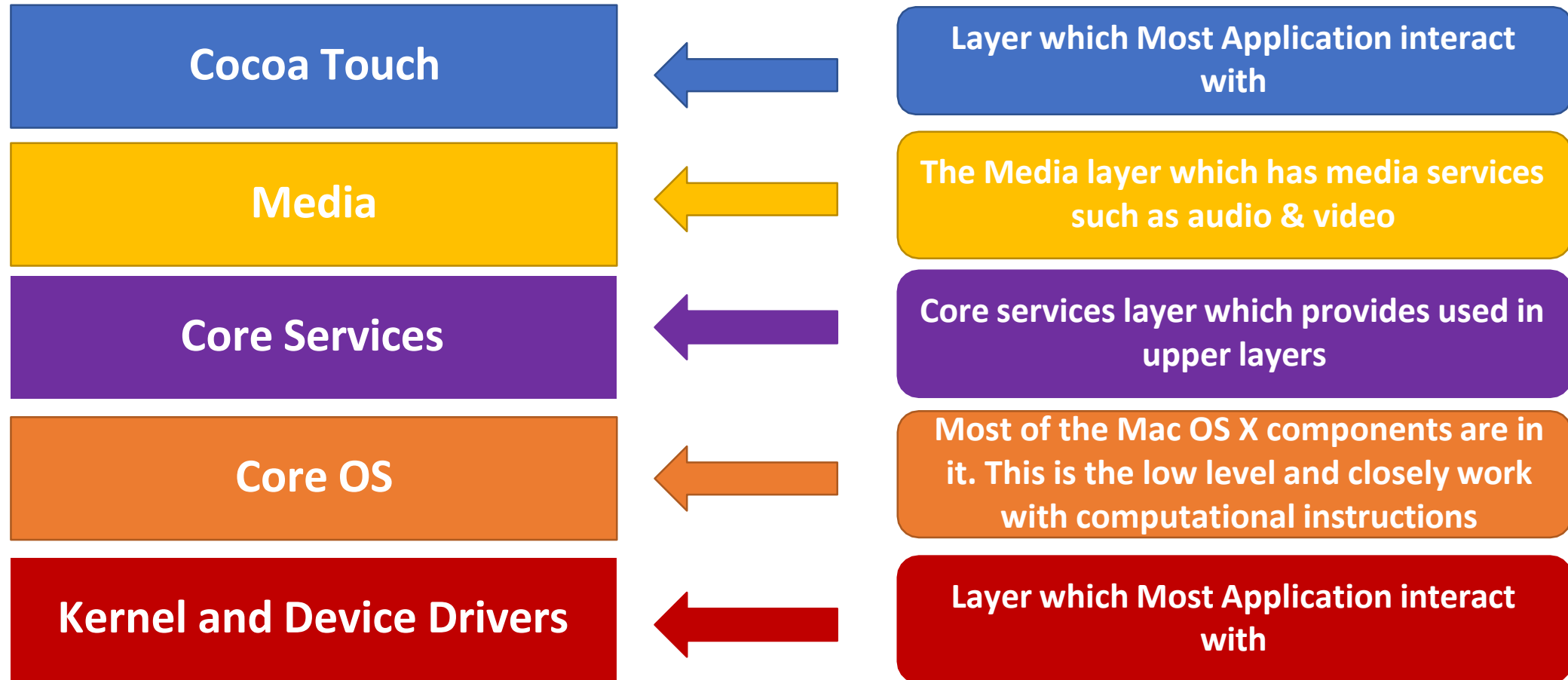


iOS Architecture

- Both the Mac OS X and iOS evolved from an earlier Apple operating system called Darwin
- Darwin is a Berkeley Software Distribution (BSD) Unix OS
- It is a discontinued operating system based on Research Unix
- iOS is a proprietary mobile operating system owned by Apple and it is only allowed to be installed in Apple equipment or devices
- Mobile operating systems such as Android and iOS are based on UNIX-like operating systems
- Linux is a family of open-source Unix-like operating systems



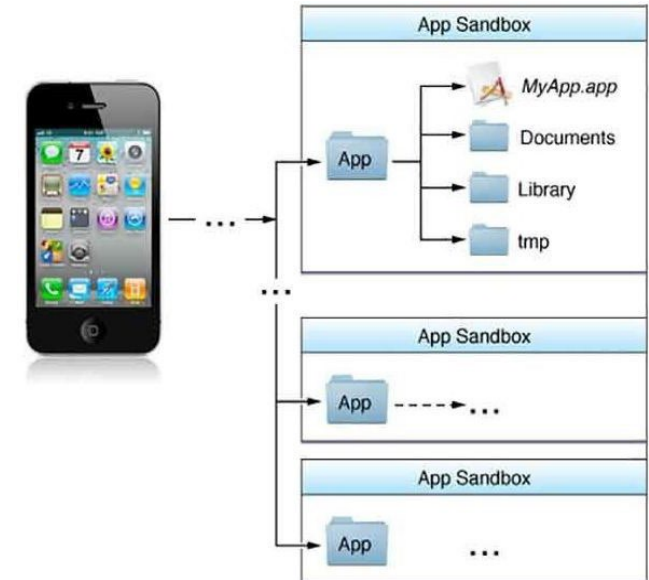
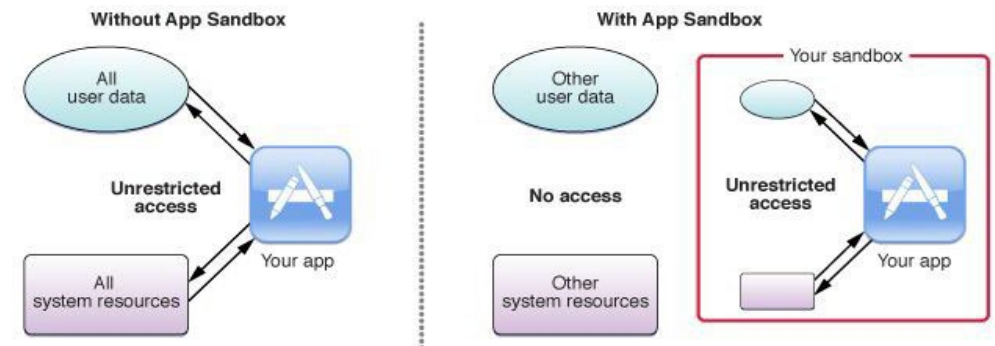
iOS Architecture (Cont'd)



App Interaction with iOS

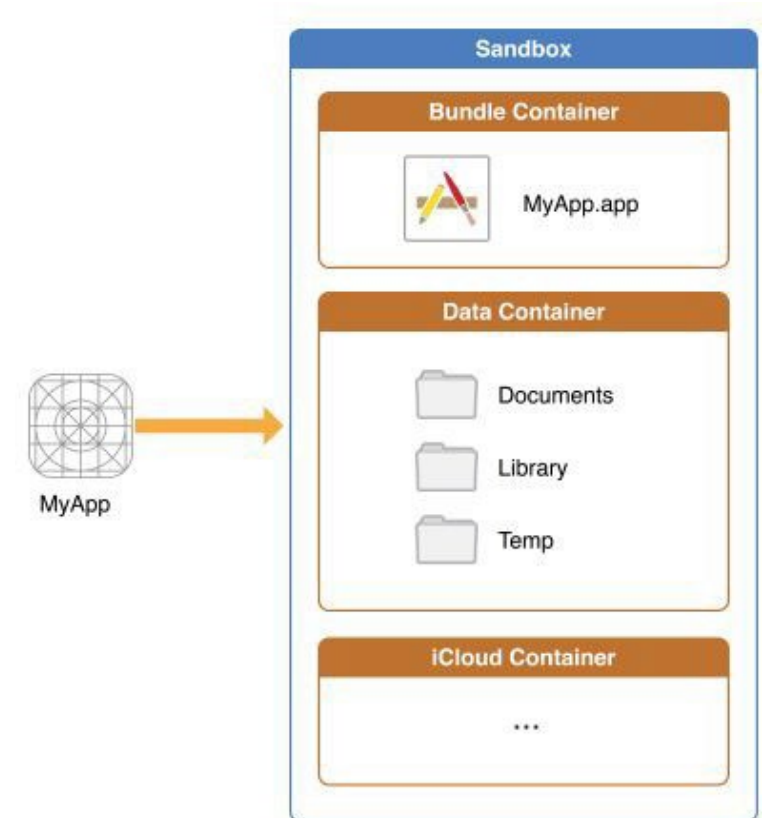


- Sandboxing, a technology whose primary job is security and control
- By enforcing a very strict set of rules on which apps can be installed on a device and exactly what they can do
- Minimum set of privileges it needs to get its job done



iOS Standard Directories: Where Files Reside

Directory	Description
AppName.app	<ul style="list-style-type: none">This directory contains the app and all of its resources
Documents/	<ul style="list-style-type: none">This directory to store user-generated content which are Userdata
Documents/Inbox	<ul style="list-style-type: none">This directory to access files that your app was asked to open by outside entities.Specifically, the Mail program places email attachments associated with your app in this directory
Library/	<ul style="list-style-type: none">The Library Directory Stores App-Specific Files such as data files, caches, resources, preferences
tmp/	<ul style="list-style-type: none">This directory to write temporary files that do not need to persist between launches of your app



IOS File System

HFS+ File system

- Apple developed Hierarchical File System (HFS)
- Provides large data sets
- Disk formatted with HFS has 512-byte Blocks at Physical level
- There are two (2) types of Blocks in the HFS system
 - **Logical Blocks**, which are numbered from first to last within the volume
 - **Allocation blocks** are a group of logical blocks used to track data. Allocation blocks, Can be tied together as groups to be utilized more efficiently by HFS



IOS File System (Cont'd)

- HFS uses both absolute time (Local time) as well as UNIX time so one can identify the location of the system.
 - Absolute time e.g. 371589010, found in History.plist(safari)
 - UNIX time e.g. 1349896210, found in moz_cookies (firefox), global_history.dat (opera)
- HFS files system uses catalog file system to organize data
- It uses B * tree (Balanced tree) structure to organize data
- Trees are consists of nodes
- When data are added or deleted, it runs the algorithm to keep balance



IOS File System (Cont'd)



Reserved Boot Block

- first 1024 bytes are reserved boot blocks

Volume Header

- It contains information about the structure of HFS Volume. It keeps track of Catalog ID Numbering and increases it one each time file added. HFS+ volume header also contains signature “H+.”

Allocation file

- It keeps track of allocation blocks used by the file system. It basically includes a bitmap. Each bit represents the status of the allocation block. If it is set to 1, that means Allocation block is used, and if it is 0, that means allocation block is not used.

Extent Overflow file

- It consists of a pointer to the extent of the. If the file is larger than eight contiguous allocation blocks, then it uses extents.

Catalog File

- It organizes data using balanced tree system as mentioned previously. It utilizes to find the location of file or folder within the volume. It also contains the metadata of file like creation and modification date, permissions.

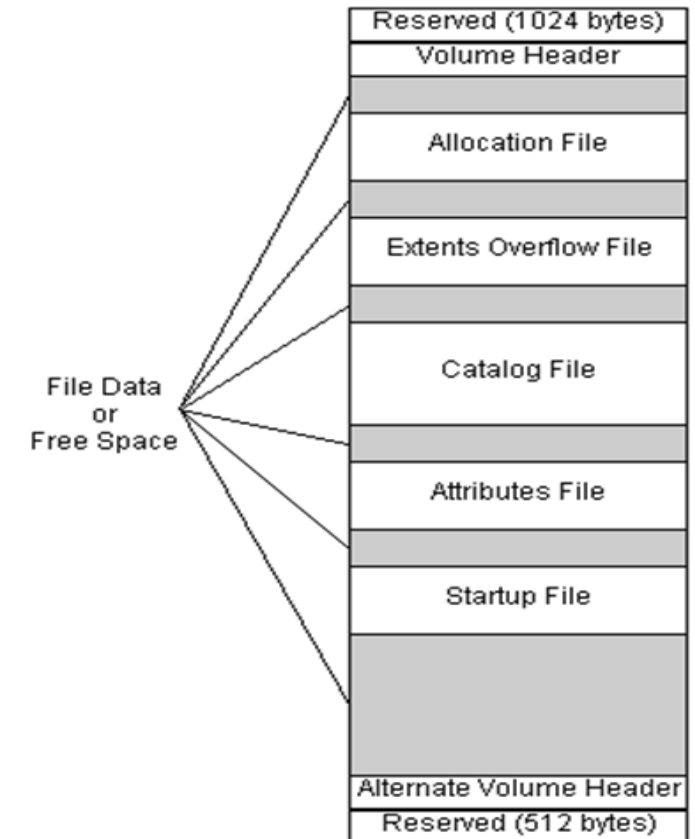


Figure. Structure of HFS+ File system

IOS File System (Cont'd)

Attribute File

- It contains the customizable attributes of a file.

Startup File

- It assists the booting system which does not have built-in ROM support.
- Actual data is stored in the file system and tracked by the file system.

Alternate Volume Header

- It is Back up Volume header located at Last 1024 byte of the volume

Last 512 Bytes are reserved

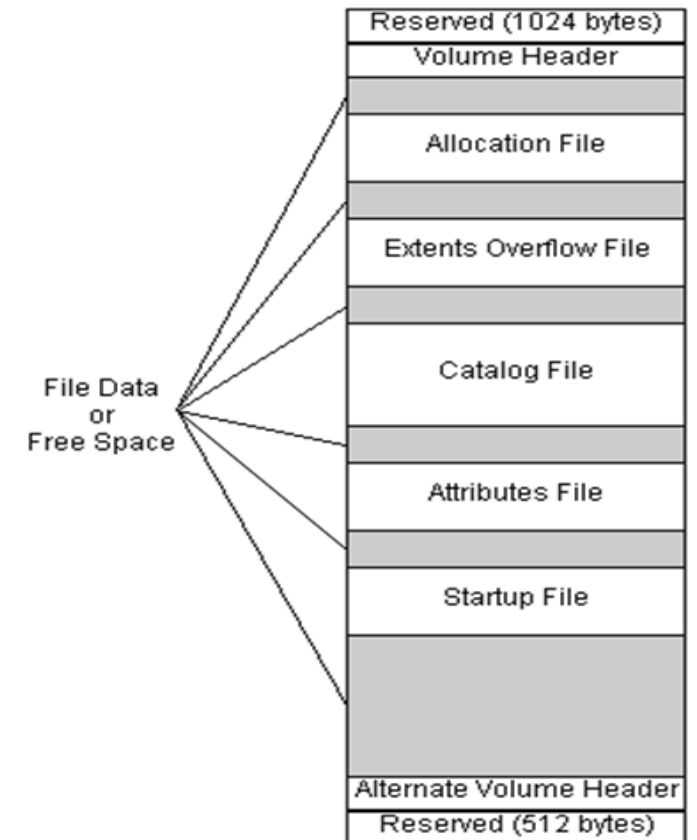


Figure. Structure of HFS+ File system

Partitions

An iOS device will have two (2) partitions:

- System partition
- Data Partition

System Partition

- Firmware/OS partitions
- Read only partition
- Containing only system files, upgrade files and basic applications



Partitions (Cont'd)

Data Partition

- Contains user data
- This partition will be the focus of most Investigation
- It is Read/Write partition
- This partition is where all iTunes applications will reside along with the user's profile data



Partitions (Cont'd)



Data Partition

Keychains	Keychain.db, which contains user password from various applications
LogsGeneral.log	General.log The OS version and Serial number Lockdown.log – Lockdown Daemon log
Mobile	User Data
Preferences	System Configurations
Run	System Logs
Tmp	Manifest.Plist , Plist Back up
Root	Caches, Lockdown, and Preferences
Property List Files	Other Plist Files residing in different locations for different applications

Property List (Plist)



- Plist is a data file (sometimes called a property file) used to store various types of data on iOS and Macintosh operating systems.
- Originally Apple used the NeXSTEP format or a binary format for these files but this was deprecated and a new XML format was introduced
- Property lists/XML files are used in the management of configuration of OS and applications
- Contains useful artifacts related to web cookies, email accounts, GPS Map routes and searches system configuration preferences, browsing history and bookmarks etc.
- These files could be open to the simple text editor to view the contents

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>EthernetBuiltIn</key>
  <string>y</string>
  <key>Timeout</key>
  <string>5</string>
  <key>ForceHPET</key>
  <string>n</string>
  <key>GUI</key>
  <string>y</string>
  <key>Default Partition</key>
  <string>hd(0,2)</string>
  <key>Graphics Mode</key>
  <string>1024x600x32</string>
  <key>GraphicsEnabler</key>
  <string>n</string>
  <key>Kernel</key>
  <string>mach_kernel_atom2</string>
  <key>Kernel Flags</key>
  <string>arch=i386</string>
</dict>
</plist>
```

SQL Lite Databases

- SQLite data format is a popular format for mobile devices and open source applications.
- Logical extraction of the iPhone could provide lots of SQLite database files
- It uses SQLite databases to store user data, the tool SQLite browser is used to explore and read SQL Lite database
- It can be downloaded from <http://sqlitebrowser.org/>
- Native iOS applications such as Calendar, Text Messages, Notes, Photos, Address Book utilize this database structure to store and organize their data



Exif Metadata

Exchangeable image file (EXIF)

- A standard that specifies the formats for images, sounds, used by digital cameras, scanners and other systems handling image and sound files recorded by digital cameras or voice recorders
- Contains, Timestamps, Longitude, latitude, location and device information depending on the device used to capture



File Name	Canon.jpg
Camera Model Name	Canon EOS DIGITAL REBEL
Date/Time Original	2003:12:04 06:46:52
Shooting Mode	Bulb
Shutter Speed	4
Aperture	14.0
Metering Mode	Center-weighted average
Exposure Compensation	0
ISO	100
Lens	18.0 - 55.0 mm
Focal Length	34.0 mm
Image Size	8x8
Quality	RAW
Flash	No Flash
White Balance	Auto
Focus Mode	Manual Focus (3)
Contrast	+1
Sharpness	+1
Saturation	+1
Color Tone	Normal
Color Space	sRGB
File Size	2.6 kB
File Number	118-1861
Drive Mode	Continuous Shooting
Owner Name	Phil Harvey
Serial Number	0560018150

Data Structure and Artifacts

- Important artifacts which are generated by features of the system or interaction of the user with the device
- It is very necessary to understand how data are stored in device
- The iOS directory structure is common across all iOS devices
- The folder structure resembles a UNIX layout and there are several directories the examiner will immediately be interested in
- Some files will be stored in text format and easily readable
- Other files will be stored in SQLite databases, XML files or binary format



Data Structure and Artifacts (Cont'd)

Timestamps

- An iOS device will have many Sqlite and plist files that can build a case for a forensic examiner
- The iOS operating system provides MACB (modified, accessed, changed, born date) times and can be vital when used with a timeline
- Timelines are an essential element for forensic analysis and in the digital world and time stamps are recorded for many events
- The Apple Core Foundation Absolute Time (CFAbsoluteTime) is also known as Mac Absolute Time or Apple Cocoa Core Data Time.
- Timestamp e.g 1615775963
- <https://www.epochconverter.com/> or Dcode (<https://www.digital-detective.net/dcode/>)



Data Structure and Artifacts (Cont'd)

Applications

- The default applications store their data in the **private/var/mobile/Library** folder
- This includes the Address Book, Mail, Calendar, Maps, Notes, YouTube, Safari, Messages, Weather and Voicemail applications
- Downloaded applications from iTunes, user data are stored under **/private/var/mobile/** or **/User/**
 - Example: **/private/var/mobile/Application** or **/User/Application**
 - This directory will hold the files associated with each application
 - assigned a 32 character alphanumeric universally unique identifier by Apple
(Example: **/User/Applications/GA07A3WW- 0E39-33OJ-B947-9CAA16688G22**) -UUID
 - unique ID will be consistent across all iOS devices



Data Structure and Artifacts (Cont'd)



Applications

<Application_Home>/AppName.app	This file contains application bundle. This file doesn't get backed up
<Application_Home>/Documents/	This folder contains application related data files
<Application_Home>/Library/	It holds application specific files
<Application_Home>/Library/Preferences/	This directory contains application preference files.
<Application_Home>/Library/Caches/	This folder holds Application specific support file and doesn't get backed up
<Application_Home>/tmp/	This folder contains temporary files.

Data Structure and Artifacts (Cont'd)

Applications

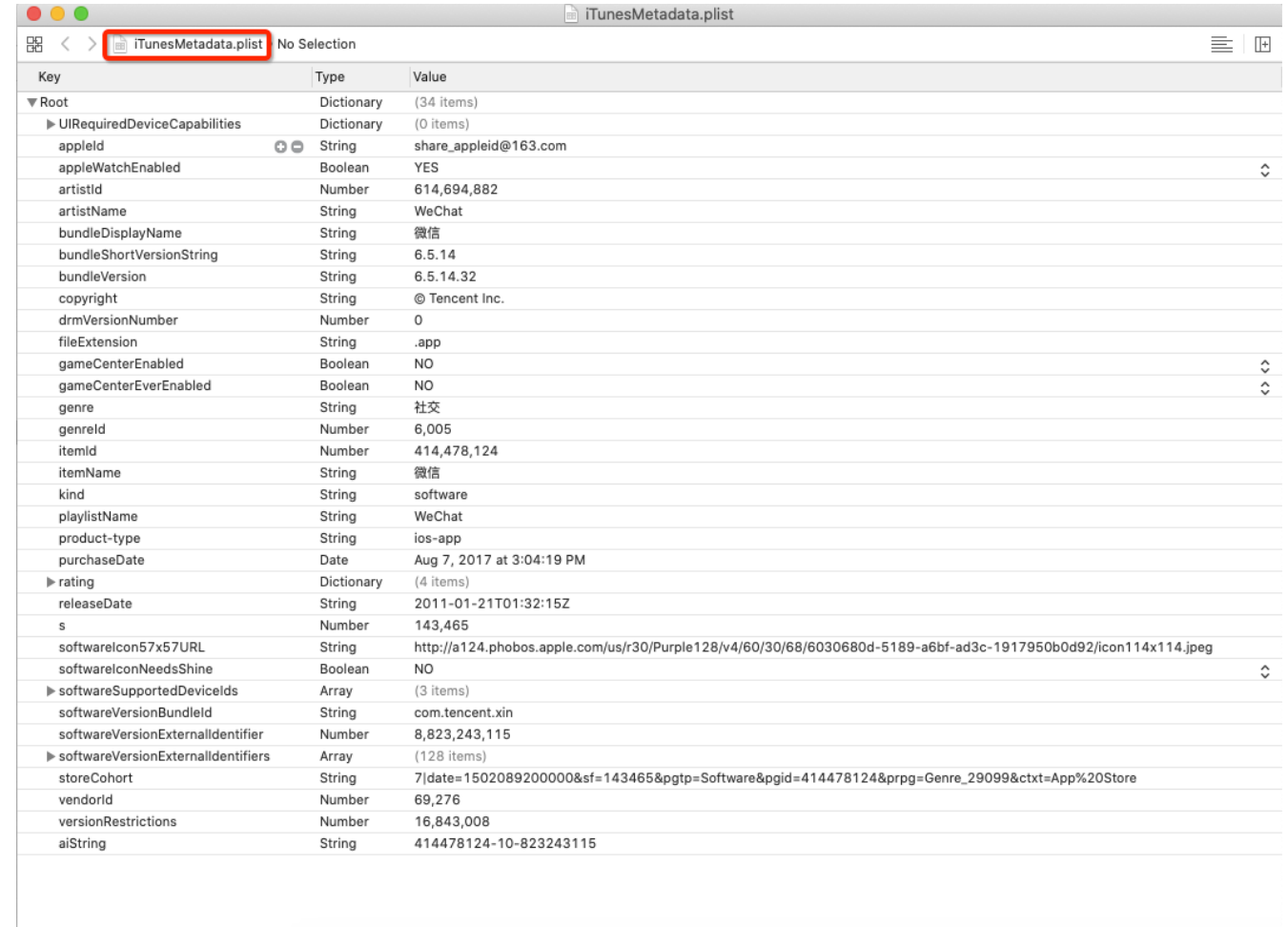
- Common files are found within most applications folders such as **info.plist**, **resourcerules.plist** and **applestores.db**.
- Depending on the application, varying configuration files, plist files and XML data will be found.
- The examiner can occasionally find username and password data, cookies, or images that will help provide evidence



Data Structure and Artifacts (Cont'd)

Applications

- iTunesMetadata.plist from the root application folder contains information related to device, **Apple account name, date of purchase** etc.



Key	Type	Value
▼ Root	Dictionary	(34 items)
▶ UIRequiredDeviceCapabilities	Dictionary	(0 items)
appleid	String	share_appleid@163.com
appleWatchEnabled	Boolean	YES
artistId	Number	614,694,882
artistName	String	WeChat
bundleDisplayName	String	微信
bundleShortVersionString	String	6.5.14
bundleVersion	String	6.5.14.32
copyright	String	© Tencent Inc.
drmVersionNumber	Number	0
fileExtension	String	.app
gameCenterEnabled	Boolean	NO
gameCenterEverEnabled	Boolean	NO
genre	String	社交
genreId	Number	6,005
itemId	Number	414,478,124
itemName	String	微信
kind	String	software
playlistName	String	WeChat
product-type	String	ios-app
purchaseDate	Date	Aug 7, 2017 at 3:04:19 PM
▶ rating	Dictionary	(4 items)
releaseDate	String	2011-01-21T01:32:15Z
s	Number	143,465
softwareIcon57x57URL	String	http://a124.phobos.apple.com/us/r30/Purple128/v4/60/30/68/6030680d-5189-a6bf-ad3c-1917950b0d92/icon114x114.jpeg
softwareIconNeedsShine	Boolean	NO
▶ softwareSupportedDeviceIds	Array	(3 items)
softwareVersionBundleId	String	com.tencent.xin
softwareVersionExternalIdentifier	Number	8,823,243,115
▶ softwareVersionExternalIdentifiers	Array	(128 items)
storeCohort	String	7[date=1502089200000&sf=143465&pgtp=Software&pgid=414478124&prpg=Genre_29099&ctxt=App%20Store
vendorId	Number	69,276
versionRestrictions	Number	16,843,008
aiString	String	414478124-10-823243115

Data Structure and Artifacts (Cont'd)

iTunes Backup

- Inside the backup folder there are several interesting files that will provide information on whether the examiner is reviewing the correct iOS device
- The root of the backup folder will contain the **status**, **info** and **manifest** plist files.

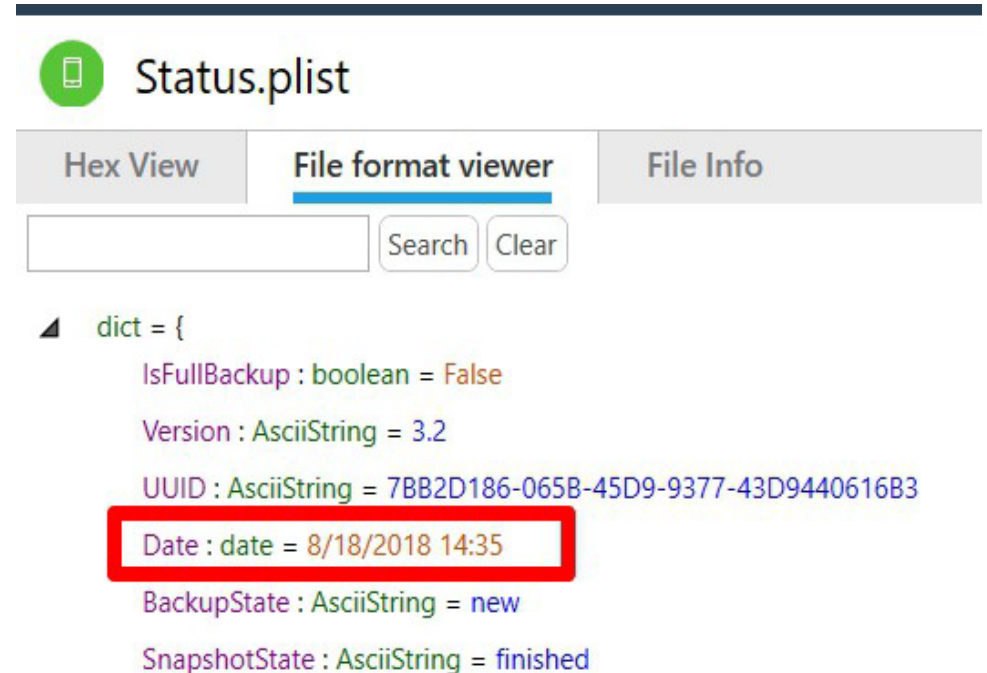


Data Structure and Artifacts (Cont'd)

The **Status.plist** provides data about the latest backup.

Consists fields:

- **IsFullBackup**: This identifies whether or not the backup was a full backup of the device
- **UUID**: This is the Universally Unique Identifier (UUID) of the device
- **Date**: This is the timestamp of the last time the backup was modified
- **BackupState**: This identifies whether the backup is a new backup or one that has been updated
- **SnapshotState**: This identifies whether the backup process has successfully finished



Data Structure and Artifacts (Cont'd)

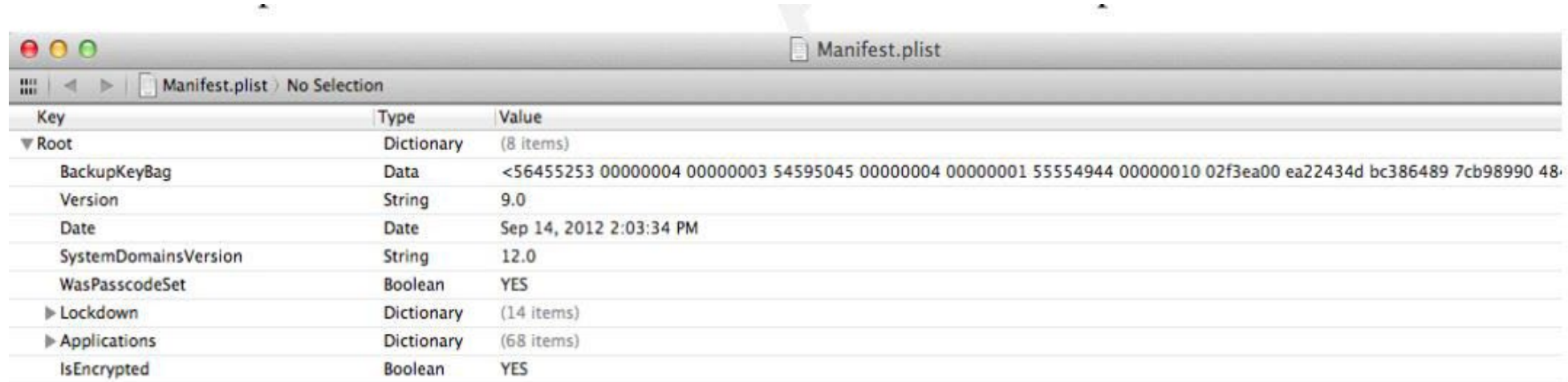
- The **Info.plist** file contains data that can be used to confirm the backup matches the device.
- The IMEI number can be found here along with the phone number



Key	Type	Value
▼ Information Property List	Dictionary	(19 items)
Build Version	String	9B206
Device Name	String	tim's iPhone
Display Name	String	tim's iPhone
GUID	String	99999999999999999999999999999999
ICCID	String	99999999999999999999999999999999
IMEI	String	99999999999999999999999999999999
Last Backup Date	Date	
MEID	String	99999999999999999999999999999999
Phone Number	String	(281) 217-5671
Product Type	String	iPhone4,1
Product Version	String	5.1.1
Serial Number	String	C38GJ25XDTC1
► Sync Settings	Dictionary	(5 items)
Target Identifier	String	b3f2cf9bdb3f2cf9bd29 b3f2cf9bd'3c8
Target Type	String	Device
Unique Identifier	String	B3F2CF9BDF4b3f2cf9bd1FC6D2C29b3f2cf9bd73
► iTunes Files	Dictionary	(7 items)
► iTunes Settings	Dictionary	(2 items)
iTunes Version	String	10.6.3

Data Structure and Artifacts (Cont'd)

- The **Manifest.plist** file contains metadata about the backed up files.



Key	Type	Value
▼ Root	Dictionary	(8 items)
BackupKeyBag	Data	<56455253 00000004 00000003 54595045 00000004 00000001 55554944 00000010 02f3ea00 ea22434d bc386489 7cb98990 48...
Version	String	9.0
Date	Date	Sep 14, 2012 2:03:34 PM
SystemDomainsVersion	String	12.0
WasPasscodeSet	Boolean	YES
▶ Lockdown	Dictionary	(14 items)
▶ Applications	Dictionary	(68 items)
IsEncrypted	Boolean	YES



Data Structure and Artifacts (Cont'd)



Photos

- Photos in **private/var/mobile/media/DCIM**
- This folder will contain photos either taken or synced to the device
- The pictures found here will have timestamp metadata
- Photos within the **100APPLE folder** indicate that they were taken from the device itself
- The camera application numbers the images from the iOS device sequentially
- The first picture taken will be named IMG_0001 and will continue numbering without regards to files being deleted or moved

Data Structure and Artifacts (Cont'd)



Keystrokes

- Keystrokes in /private/var/mobile/Library/Keyboard
- The dynamic dictionary is the text file dynamic-text.dat
- This dictionary stores words typed by the user during the course of using the device.
- Any word entered into applications like Notes, Safari, Messages, Facebook or any application that will allow text input, will be captured
- Intent is to aid user in typing thus technical or special keywords that may not be Standard English words or acronyms that could be helpful for the investigation

Data Structure and Artifacts (Cont'd)

Passwords



- Passwords in /private/var/Keychains
- iOS applications use Apple's keychain for password management
- Contains key-chain-2.db file
- Accounts and passwords such as Voicemail passwords, wireless access point key phrases and device login passcodes can be found inside this database
- In some cases the passwords will be encrypted by the iOS encryption keychain procedure and will need 3rd Party Tools to be decrypted

Data Structure and Artifacts (Cont'd)

Notes

- Notes in /private/var/mobile/Library/Notes
- Review acronym or keywords that may be useful to investigation

Text Messages

- /private/var/mobile/Library/SMS the sms.db can be found
- Review text messaging communication



Data Structure and Artifacts (Cont'd)

Browser Cookies

- Browser Cookies in /private/var/mobile/Library
- Safari cookies can be an important piece of evidence when identifying web browsing activities from the device



Data Structure and Artifacts (Cont'd)

Browser Cache

- Browser Searches in /private/var/mobile/Library/Caches/Safari
- Search terms from using the Safari browser can be found in the **RecentSearches.plist** file
- This particular plist file is in XML format and can be read with a text viewer.



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>RecentSearches</key>
  <array>
    <string>corvette emergency brake line diagram
</string>
    <string>who won the debate</string>
  </array>
</dict>
</plist>
```

Data Structure and Artifacts (Cont'd)

AddressBook

- AddressBook in /private/var/mobile/Library/AddressBook
- The AddressBook.sqlitedb file in the iOS can contain a wealth of information about the owner's personal contacts



Data Structure and Artifacts (Cont'd)

Call History

- Call History in /private/var/Library/CallHistory
- The call history of an iOS device that can place cellular calls is contained in call_history.db



Data Structure and Artifacts (Cont'd)

Geographical Location and Wi-Fi Data

- GPS and Wi-Fi evidence can be a sought after item to help build a picture of the iOS device location at a specific time and also users habits
- Many iOS applications will attempt to cache the user's location and store GPS data depending on the purpose of the application
- example iPhone's camera will attempt to store longitude and latitude when a photo is taken



Data Structure and Artifacts (Cont'd)



- The **consolidated.db** file found in private/var/Library/Caches/locationd can hold a tremendous amount of geolocation data
- The wifilocation table contains longitude, latitude, MAC, and timestamps of wireless infrastructures the iOS device has utilized
- The cellLocationLocal table contains longitude, latitude, altitude, timestamps and tower data

	Timestamp	Latitude	Longitude	HorizontalAccuracy
40	313168432.468664	29.6521617666667	-95.1564094333334	1500.0
41	313168450.468173	29.6476963166667	-95.1566544666667	1500.0
42	313168469.464954	29.6431089833333	-95.15822785	1500.0
43	313168491.464108	29.6385277166667	-95.1617466166667	1500.0
44	313168499.472149	29.6371233333333	-95.16333835	1500.0
45	313168522.46753	29.6328585833333	-95.1681582833333	1500.0
46	313168559.465591	29.6263518333333	-95.1755349833333	1500.0
47	313168672.468137	29.6097458666667	-95.2018664333333	1500.0
48	313168681.471775	29.6085986833333	-95.2036239333334	1500.0
49	313168732.467407	29.59904035	-95.1981717333333	1500.0
50	313168772.467348	29.5913441666667	-95.19002265	1500.0
51	313168868.468044	29.5725225	-95.1715411	1500.0
52	313168896.469815	29.5665713166667	-95.1664867333333	1500.0
53	313168986.468171	29.5481764	-95.1492766166667	1500.0
54	313169017.469061	29.5417652833333	-95.1430994833333	1500.0
55	313169023.461444	29.5404842666667	-95.1418728333333	1500.0
56	313169131.471426	29.5163927833333	-95.12219825	1500.0
57	313169239.474032	29.49136835	-95.1072105666667	1500.0
58	313169243.46496	29.4904377666667	-95.1066540666667	1500.0
59	313169248.473248	29.4892832166667	-95.1059461166666	1500.0
60	313169321.463636	29.4727524333333	-95.0960381	1500.0
61	313169332.472743	29.4705507	-95.0945748	1500.0

Summary

- iOS devices collect and store a tremendous amount of evidence about a user's activities
- Understanding the fundamentals of iOS operating system, file systems, directories, data structures and artifacts
- With this forensic evidence available, and more business being conducted on iOS devices, forensic examiners can now be able to successfully and accurately pull this evidence when performing an analysis

