iPhone Processing

Introduction - Steve Whalen, CFCE

- Fifteen years of investigative experience as a trooper with the Delaware State Police
- Eight years as a Computer Forensic Examiner with the DSP High Technology Crimes Unit
- Conducted examinations on thousands of different types of digital media from hundreds of investigations since 1999
- Recognized as a Certified Forensic Computer Examiner (CFCE) though the International Association of Computer Investigative Specialists (IACIS)
- Regularly instruct other law enforcement officers both nationally and internationally in computer forensics and incident response
- Recognized as a Certified Instructor in the fields of computer forensics, law enforcement and Internet Safety education
- Founder of Phoenix Data Group, LLC and Co-founder of Forward Discovery, Inc.
- Have been dissecting computers since 1982.

Forward Discovery, Inc.

FORWARD Discovery

Forward Discovery is a global leader in computer forensics, incident response, and e-Discovery. Our team of world class experts, with extensive law enforcement and information security backgrounds, can directly assist you with your emergency and routine computer incident response needs. We also offer industry leading training in a variety of investigative and forensics areas, allowing you to bring your team's capabilities to a whole new level. From cell phone and computer forensics to network investigation and analysis, our proven specialists can provide you with the services you need on a short-term or long-term basis. Allow us to bring our international investigative and technical experience to you.

Forward Discovery was created through the merger of Digital First Discovery, The Phoenix Data Group and Meadowhawk Technologies. The staff, and expertise, of all three companies were brought together to offer you unparalleled service and support.

iPhone Processing

Outline

- Introduction to the iPhone
- iPhone Backup Files
- Unmodified vs. “Jailbroken” iPhones
- What Can Be Recovered
- iPhone Security Features

iPhone Processing

Overview

- The iPhone file system is based on Mac OSX
- Activation and management of it's contents is managed by the iTunes application on either Mac OSX or Windows
- Currently their is no known way to image its protected file system without support from Apple
- A majority of the iPhone's information is kept on the computer after a sync

iPhone Processing

Technical Specs (Original iPhone - v1)

- The iPhone Specifications:
  - 3.5 inch Color LCD Touch Screen
  - iPhone OS (OS X variant) 1.1.4
  - 620 MHz ARM CPU
  - 128 MB DRAM
  - Flash Memory Storage (4, 8 or 16GB)
  - WiFi & Edge (2.5G) Networking
  - Lithium-ion polymer Battery
  - Physical size 4.5x2.4x0.46 in
  - Weight 4.8 oz

iPhone Processing

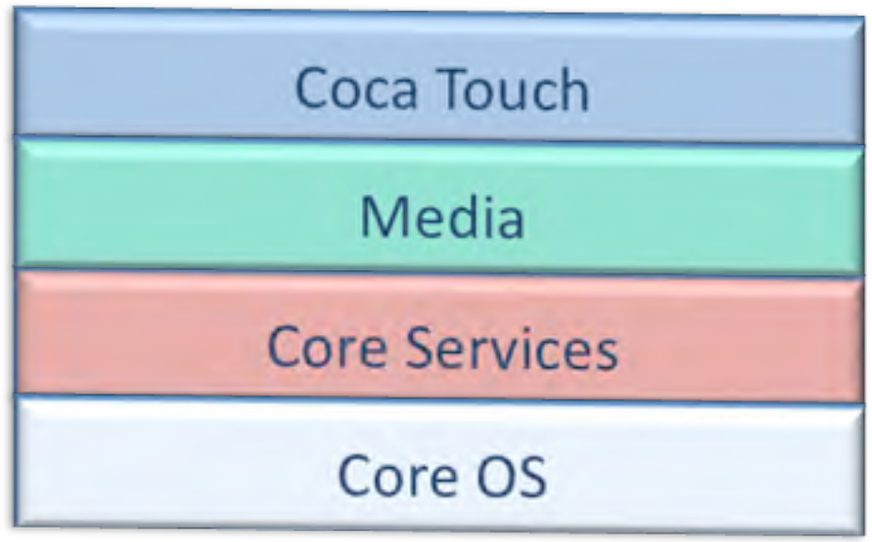
Technical Specs (iPhone3G)

- The iPhone3G Specifications:
  - 3.5 inch Color LCD Touch Screen
  - iPhone OS (OS X variant) version 2.0
  - 620 MHz ARM CPU
  - 128 MB DRAM
  - Flash Memory Storage (8 or 16GB)
  - WiFi, Edge 3G Networking
  - Assisted GPS
  - Approved thrid-party applications
  - Lithium-ion polymer Battery
  - Physical size 4.5x2.4x0.48 in
  - Weight 4.7 oz

iPhone Processing

Operating System

- The iPhone OS is a version of OS X designed especially for the phone
- Like its big brother it is a layered design
- The iPhone OS has 4 layers
  - Cocoa Touch – Application framework
  - Media – audio, video & graphics technologies
  - Core Services – Fundamental Services
  - Core OS – Kernel & driver Layer



iPhone Processing

Activation

- The iPhone must be activated via a computer that has iTunes installed.
- Once the iPhone is connected to a Mac, iTunes launches and the activation is initiated, the phone plan selected and the number assigned

iPhone Processing

Sync

- After activation, when the iPhone is connected to the computer a sync will be conducted
- The user can define what is to be Synced to include:
  - Music
  - Photos
  - Ringtones
  - Contacts & Calendars
  - Podcasts
  - Video
  - Third party applications
- Third party applications can initiate the use of the iPhone as a file storage device

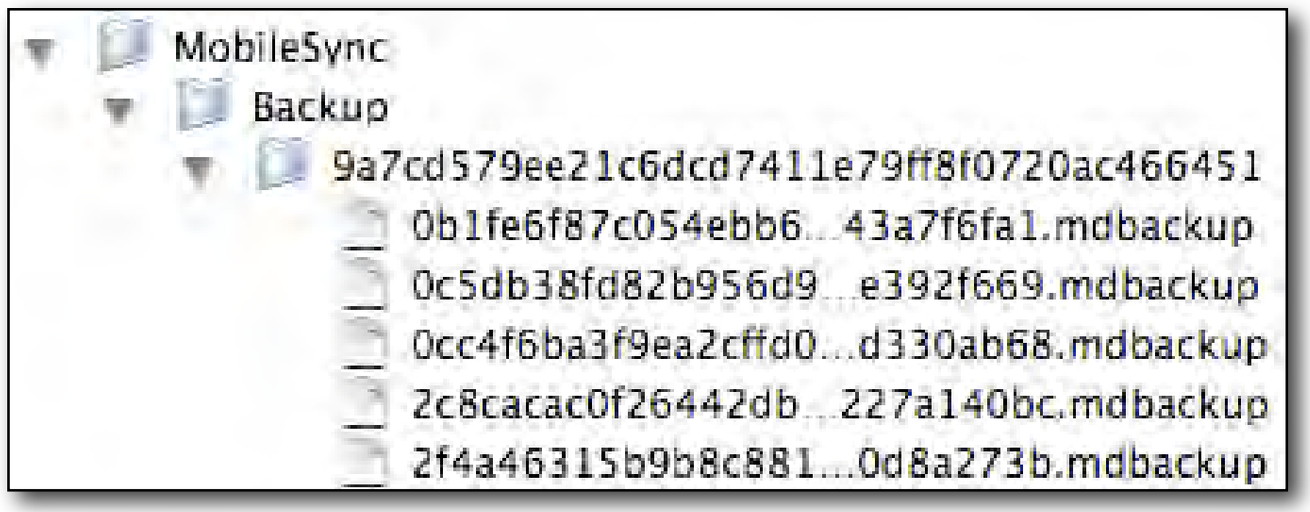
iPhone Processing

.mdbackup files

- During the sync process, the iPhone's data is backed up to the user's computer
- The backup files are located at:

  ~/Library/Application Support/MobileSync/Backup/(unique identifier)
- The files have a .mdbackup extension with a unique identifier as the name:

  0a49f42bc2fbedb5713469b34a0bb158097fc0f5.mdbackup
- The backup files are in a binary plist format and can contain encapsulated images, SQLite database files and even other plists



iPhone Processing

.mdbackup files

- The backup files can contain:
  - Safari History & Bookmarks
  - Photos (phone & synced iPhoto)
  - Sent & Received SMS
  - Calendar Events
  - Notes
  - Address Book Entries
  - Call History
  - Cookies
  - Google Map History
  - Email Account Settings
  - YouTube Last Search, Last Viewed & Bookmarks data

iPhone Processing

Processing .mdbackup files - MobileSync Browser

- MobileSync Browser is donationware that can parse through the .mdbackup files to locate:

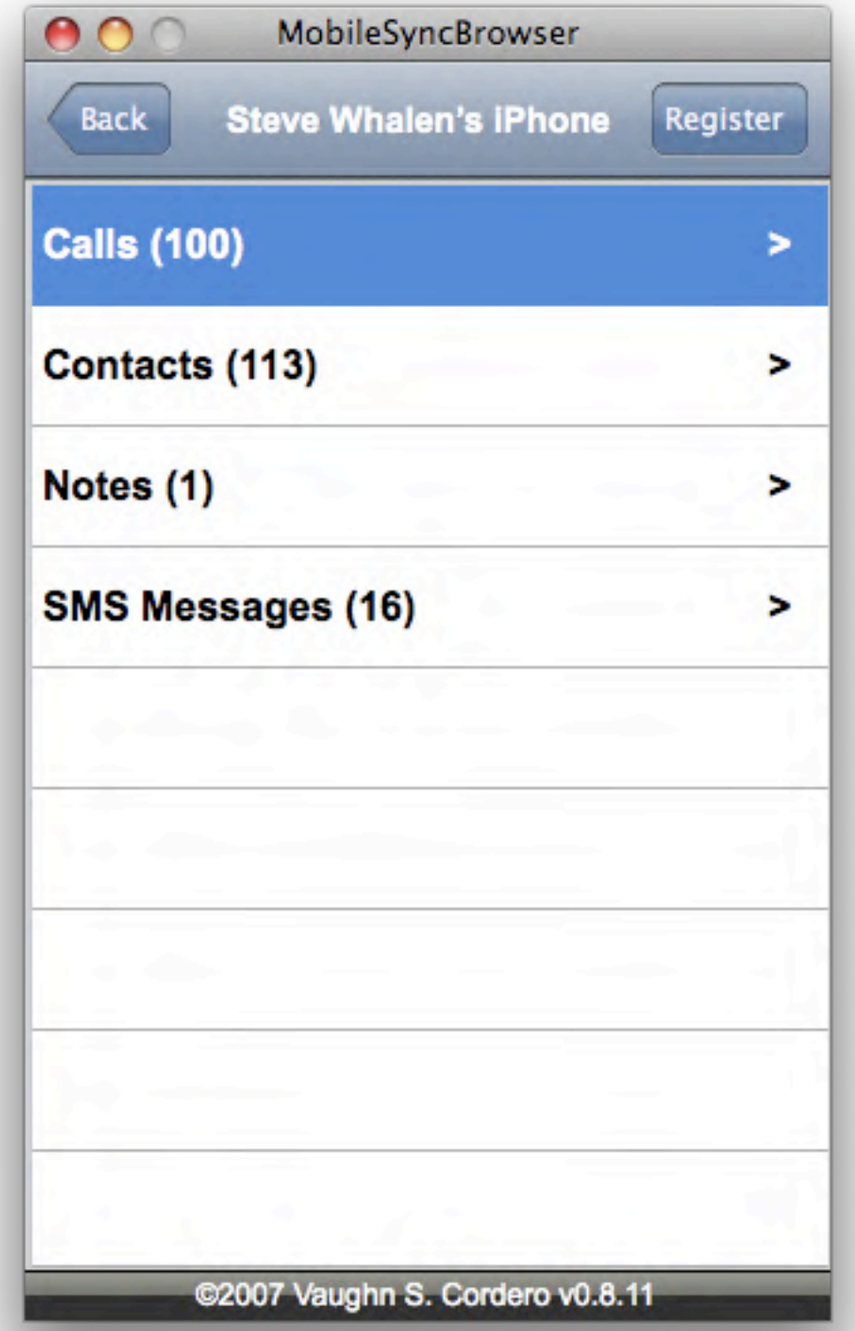
  Call records

  Contacts

  Notes

  SMS Messages

http://homepage.mac.com/vaughn/msync/



iPhone Processing

Processing .mdbackup files - extract_iphone_backup.py

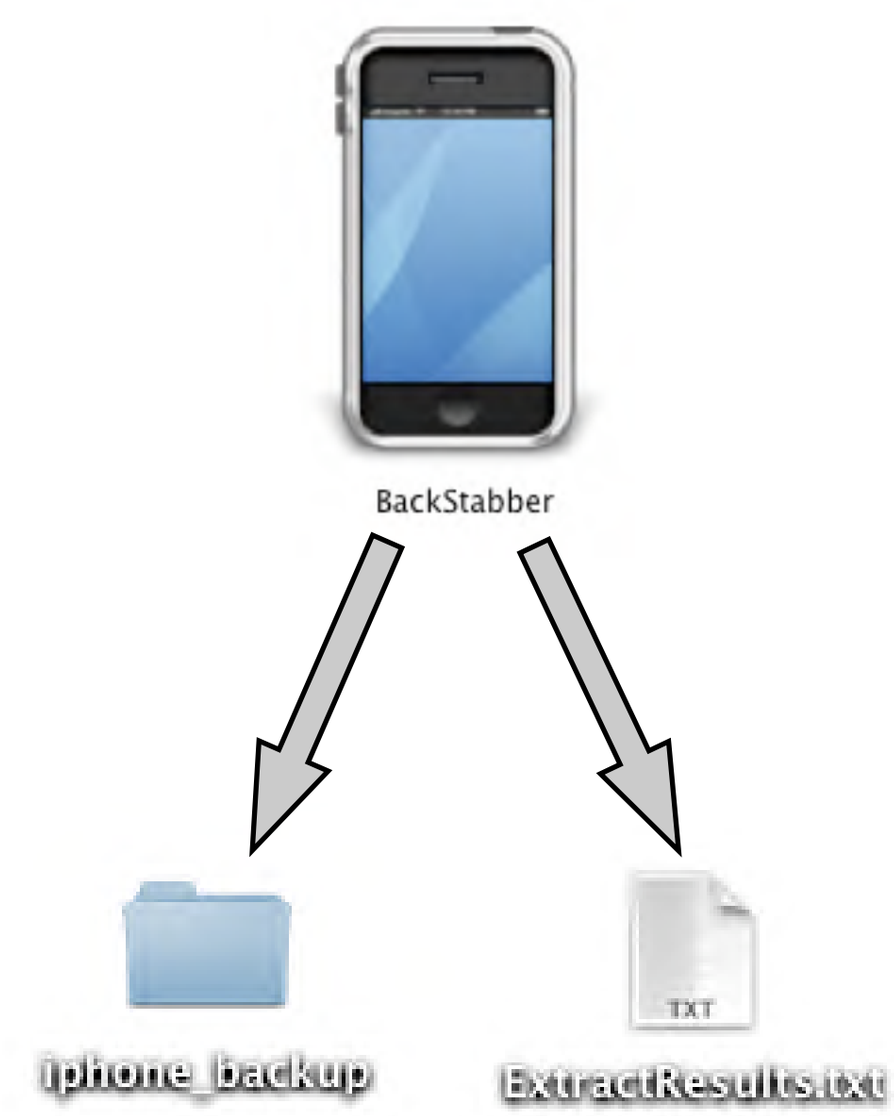
- Uninnovate.com's extract_iphone_backup.py
- A Python Script used to extract iPhone Backup data
- Extracts the data to PLISTs & SQLite databases
- Data can be viewed using viewers such as Plist Editor & SQLite DB Browser
- Some of the information that can be extracted:

  - Safari History & Bookmarks
  - Photos
  - Sent & Received SMS
  - Calendar Events
  - Notes
  - Address Book Entries
  - Call History
  - Cookies
  - Google Map History
  - Email Accounts
  - YouTube Last Search Data, Last Viewed & Bookmarks

iPhone Processing

BackStabber

- Using a variation of the extract_iphone_backup.py, Forward Discovery team member (Ryan Kubasiak) has created an application to automate the process
- BackStabber can be placed on the Desktop or in the Applications folder
- It extracts the plists and db files and places then in a folder on the desktop along with a text file that documents the extraction process



BackStabber can be downloaded from:
www.macosxforensics.com

iPhone Processing

Accessing the phone

There are basically 2 types of iPhones

- **Un-modified**
- **Jailbroken** (unshackled)
- It is estimated that 2/3 of all iPhones have been unlocked or jailbroken

iPhone Processing

Processing iPhone - Un-modified

- There are currently no methods of *forensically* analyzing an un-modified iPhone without modifying the file system
- Some utilities can retrieve a limited amount of data from un-modified iPhones
- Manually navigating through data may leave the lightest footprint
- Document by taking video, pictures and notes

iPhone

Processing iPhone - Un-modified - PhoneView

- PhoneView (previously named MegaPhone) is third party utility that allows for using the iPhone as a hard drive and allows viewing
  - Contacts
  - SMS
  - Photos
  - Call History

This is not a forensically sound process, dates and times will be changed. A folder and text file is written to the iPhone. This program can delete files. The iPhone is not recognized if a hardware write block is placed between it and the Mac.

iPhone Processing

Processing iPhone - Jailbroken

- Because the iPhone is a protected system a user must hack or “Jailbreak” the iPhone to access folders/files & add 3rd party non-sanctioned applications
- Software used to jailbreak iPhone’s are
  - Jailbreak
  - iFuntastic
  - ZiPhone
  - iLiberty

- Once the file system is accessible files or parts of the file system can be can be copied out and/or imaged using a number of different programs to include iFuntastic and applications installed via Jailbreak’s Installer.app

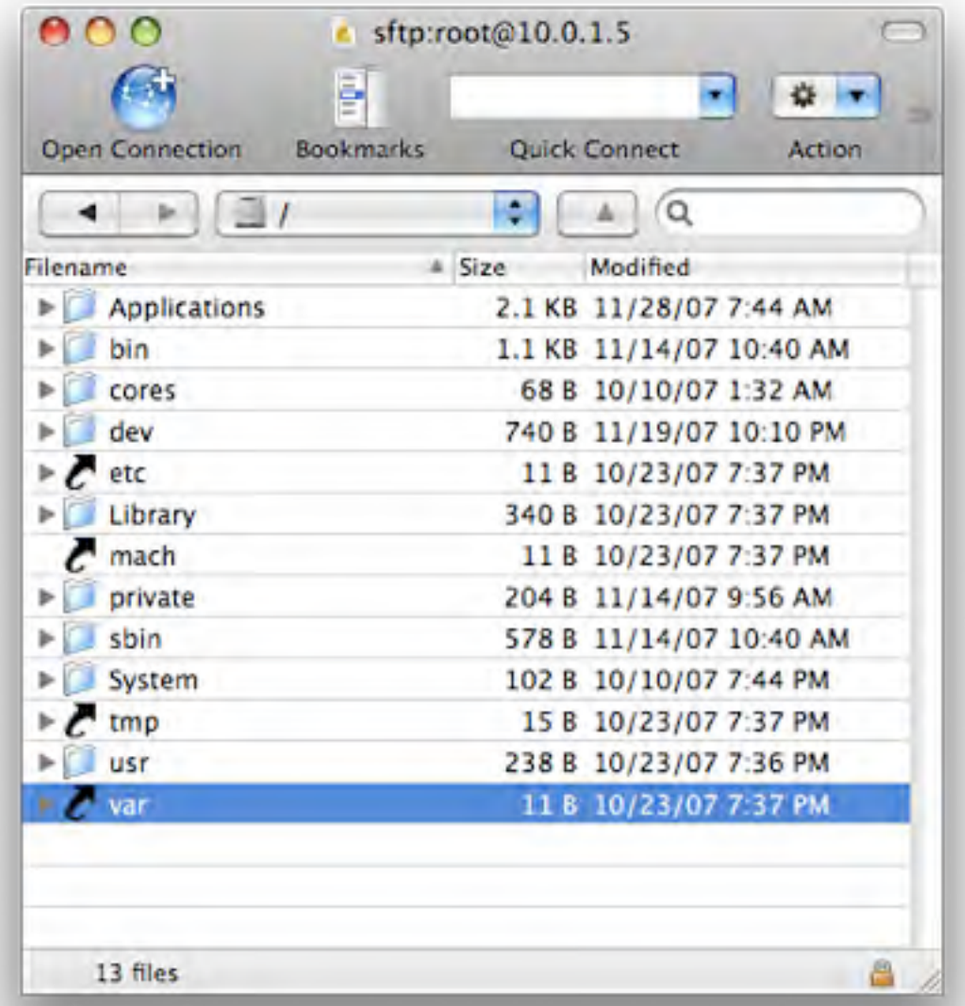
iPhone Processing

- Phones that have been unlocked by the USER offer the opportunity to view the file system.
- A jailbroken iPhone offers the user the ability to add non-santioned 3rd party apps to the phone
- Apps include
  - App Installer
  - Screen Capture
  - Games
  - Terminal (command line)
  - File Manager
  - Video Capture
  - SSH
  - VNC

iPhone Processing

Seeing What's Inside

- Some methods of Jailbreaking will install an SSH client
- An SSH client will allow data transfer from a computer to the iPhone and vise versa
- Using an SFTP client can allow GUI access to files via SSH which could then be copied out
- DD can be used to image the phone using netcat & SSH

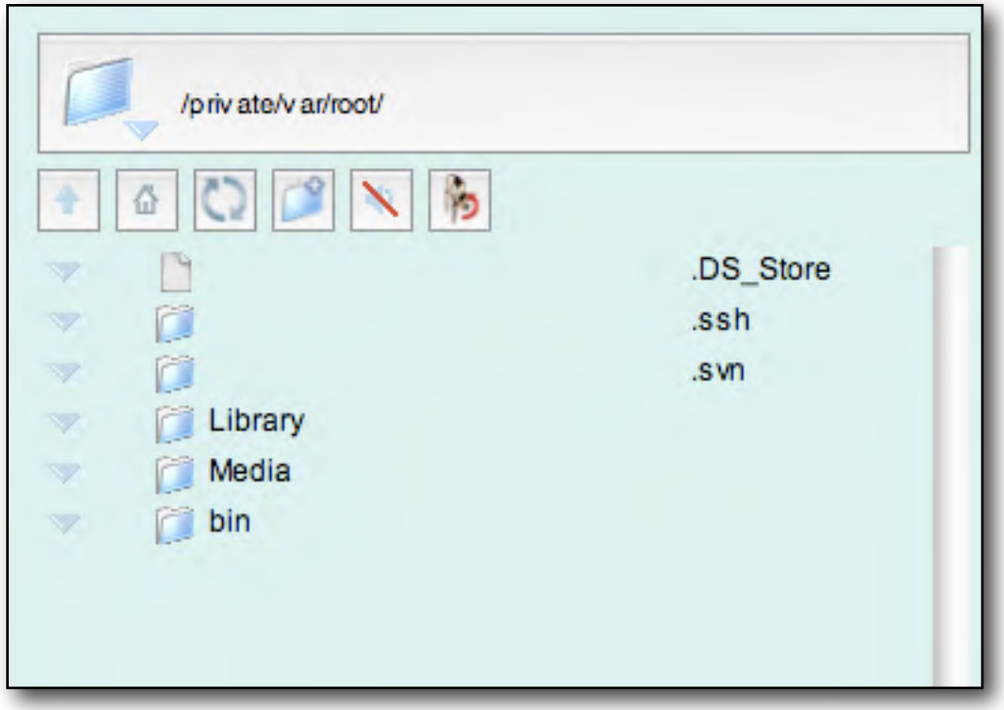


think-forensicss-macbook-pro-15:~ thinkforensics$ ssh root@10.0.1.5
root@10.0.1.5's password:
Last login: Fri Nov 16 12:52:07 2007

iPhone Processing

What Can be Recovered?

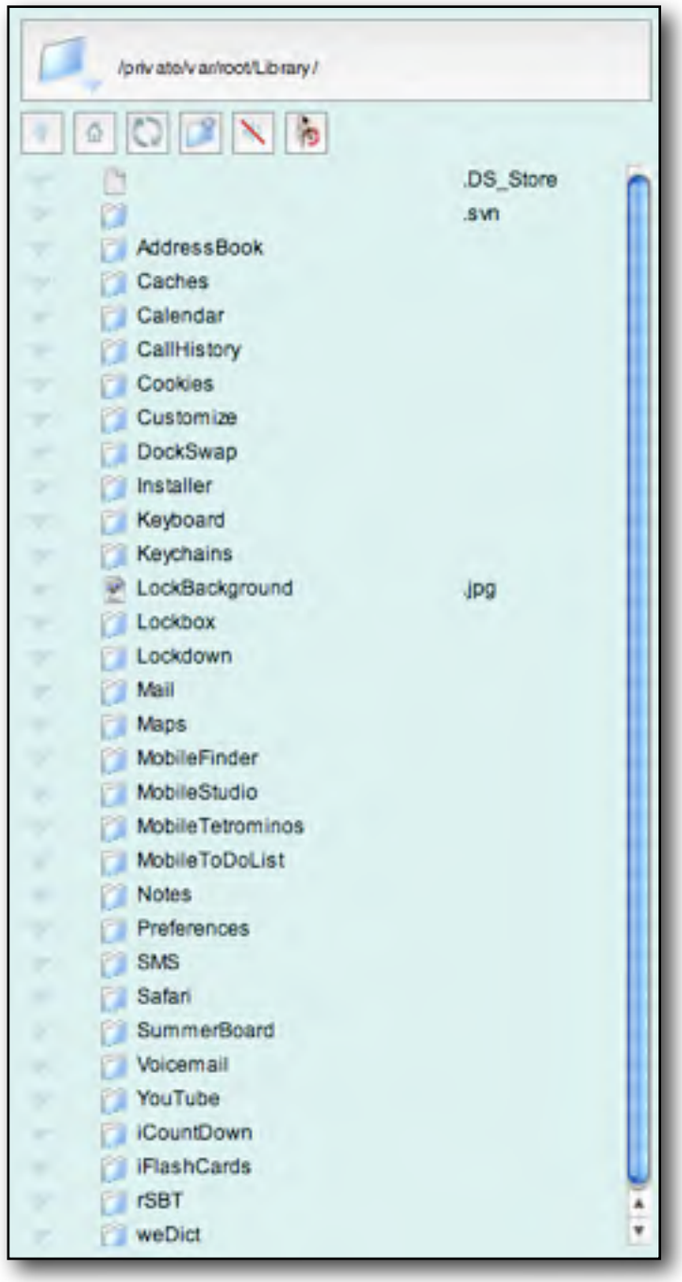
- Firmware 1.1.3 and before
  - The “user” account is called root and is located at:
    - /private/var/root
- Root’s default folders are
  - Library - Plists, DB files, Voicemail
  - Media - Images, iTunes & Ringtones
  - bin - System programs



iPhone Processing

What Can be Recovered?

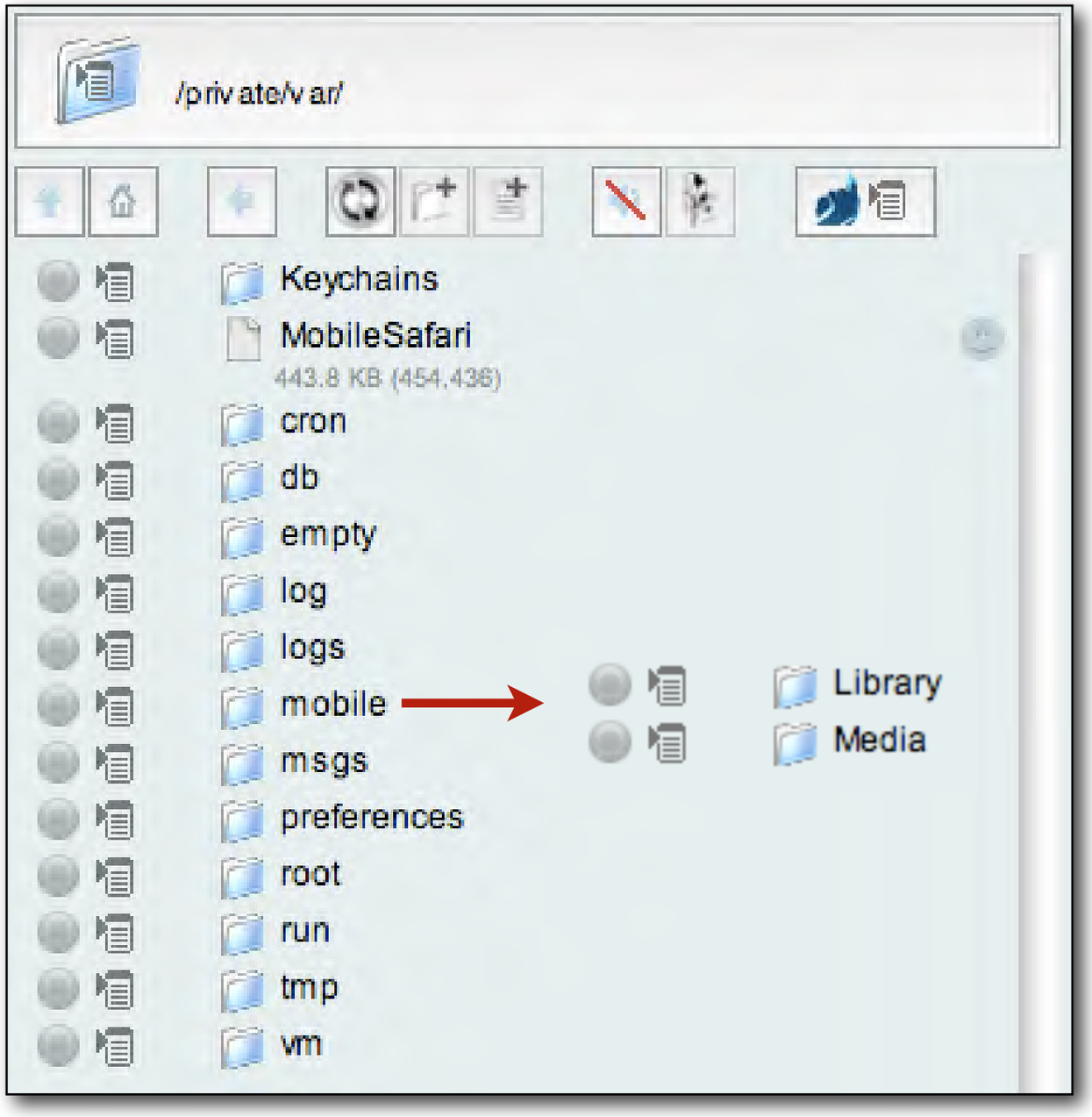
- The 1.1.3 Library folder holds a wealth of information to include
  - Web History
  - Cookies
  - Voicemail
  - SMS
  - Address book
  - Calendar
  - Call History
  - Data for Third Party Apps
- Information is contained in both Plists & DB files



iPhone Processing

What Can be Recovered?

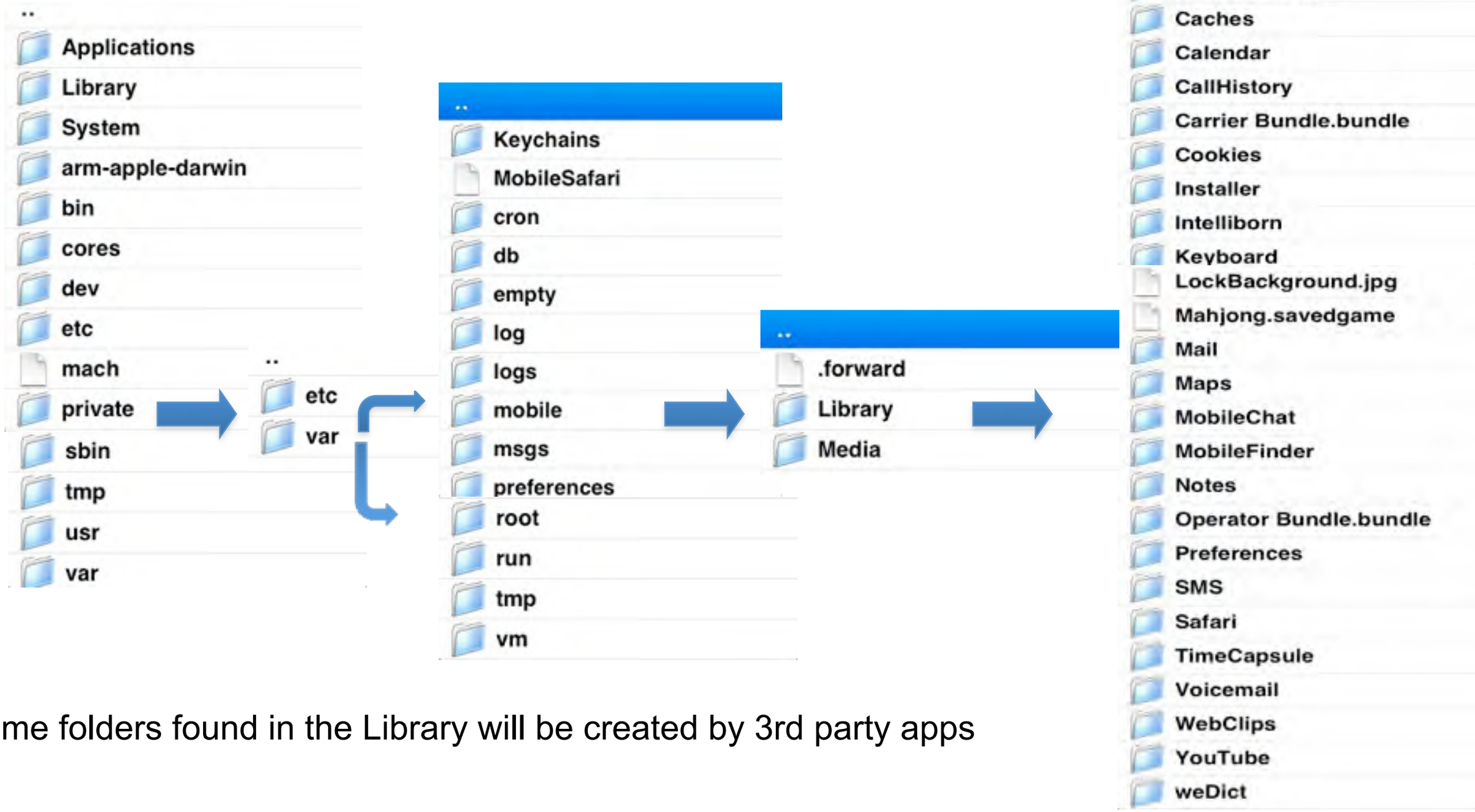
- Firmware 1.1.4 and up
  - The data previously found in the root folder is now located at:
    - /private/var/mobile
- mobile's default folders include:
  - Library - Plists, DB files, Voicemail
  - Media - Images, iTunes & Ringtones



iPhone Processing

What Can be Recovered?

versions 1.1.4 and up folder view



Some folders found in the Library will be created by 3rd party apps

iPhone Processing

What Can be Recovered?

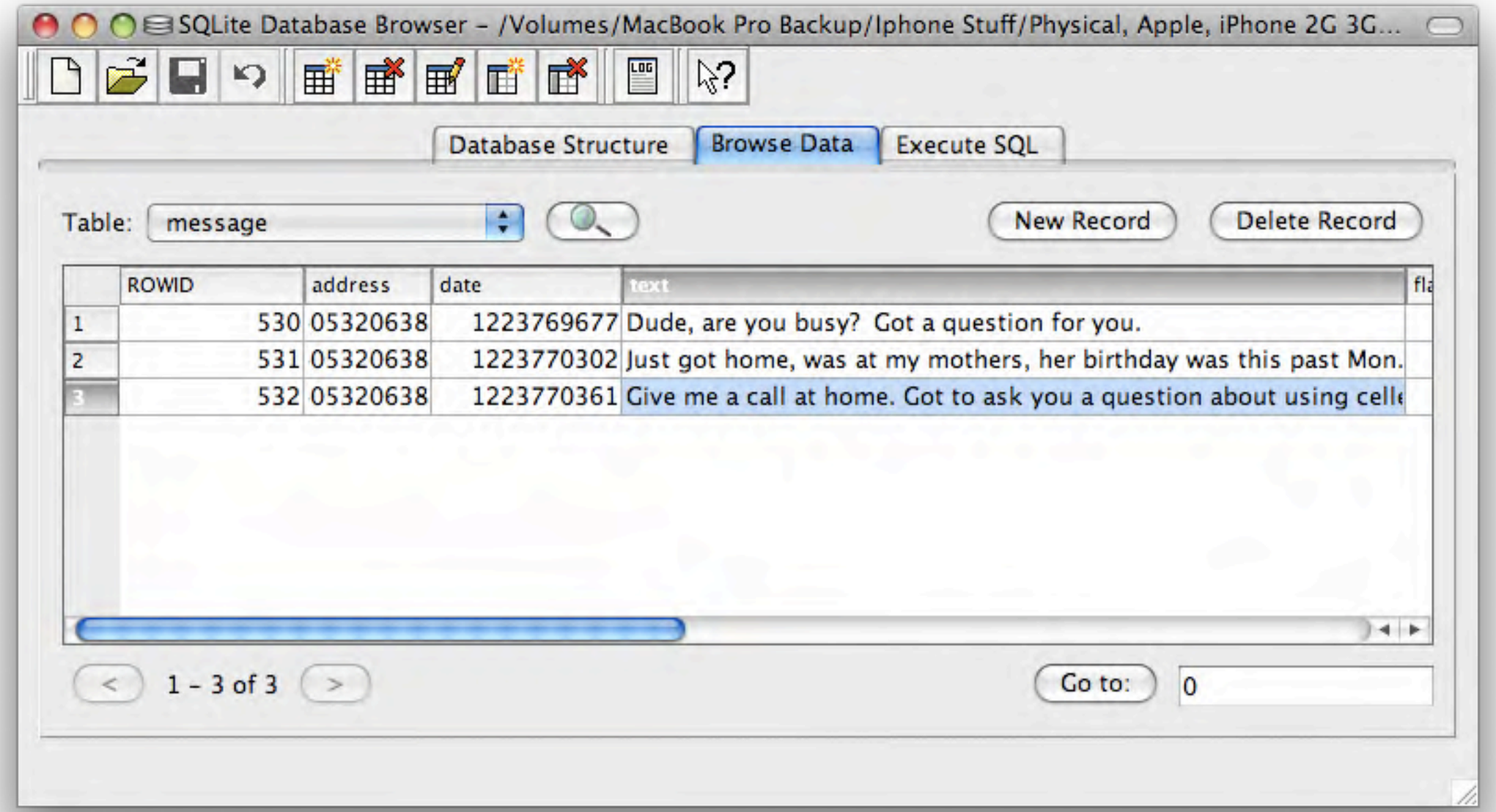
- Key files that may hold evidentiary data
- Some of these may be also be found in the backup files

/private/var/mobile/Library/CallHistory/call_history.db
/private/var/mobile/Library/AddressBook/AddressBook.sqlitedb
/private/var/mobile/Library/AddressBook/AddressbookImages.sqlitedb
/private/var/mobile/Library/Cookies/Cookies.plist
/private/var/mobile/Library/Keyboard/dynamic-text.dat
/private/var/mobile/Library/Mail/Accounts.plist
/private/var/mobile/Library/Mail/(mail account name)/Deleted Messages
/private/var/mobile/Library/Mail/(mail account name)/Sent Messages
/private/var/mobile/Library/Mail/(mail account name)/INBOX
/private/var/mobile/Library/Maps/History.plist
/private/var/mobile/Library/YouTube/Bookmarks.plist
/private/var/mobile/Library/Voicemail/(amr files)
/private/var/mobile/Library/Voicemail/voicemail.db
/private/var/mobile/Library/Safari/Bookmarks.plist
/private/var/mobile/Library/Safari/History.plist
/private/var/mobile/Library/Suspend.plist
/private/var/mobile/Library/Safari/SuspendState.plist
/private/var/mobile/Library/Safari/SMS/sms.db
/private/var/mobile/Library/Preference/(various preference Plists)
/private/var/mobile/Library/Notes/notes.db

iPhone Processing

What Can be Recovered?

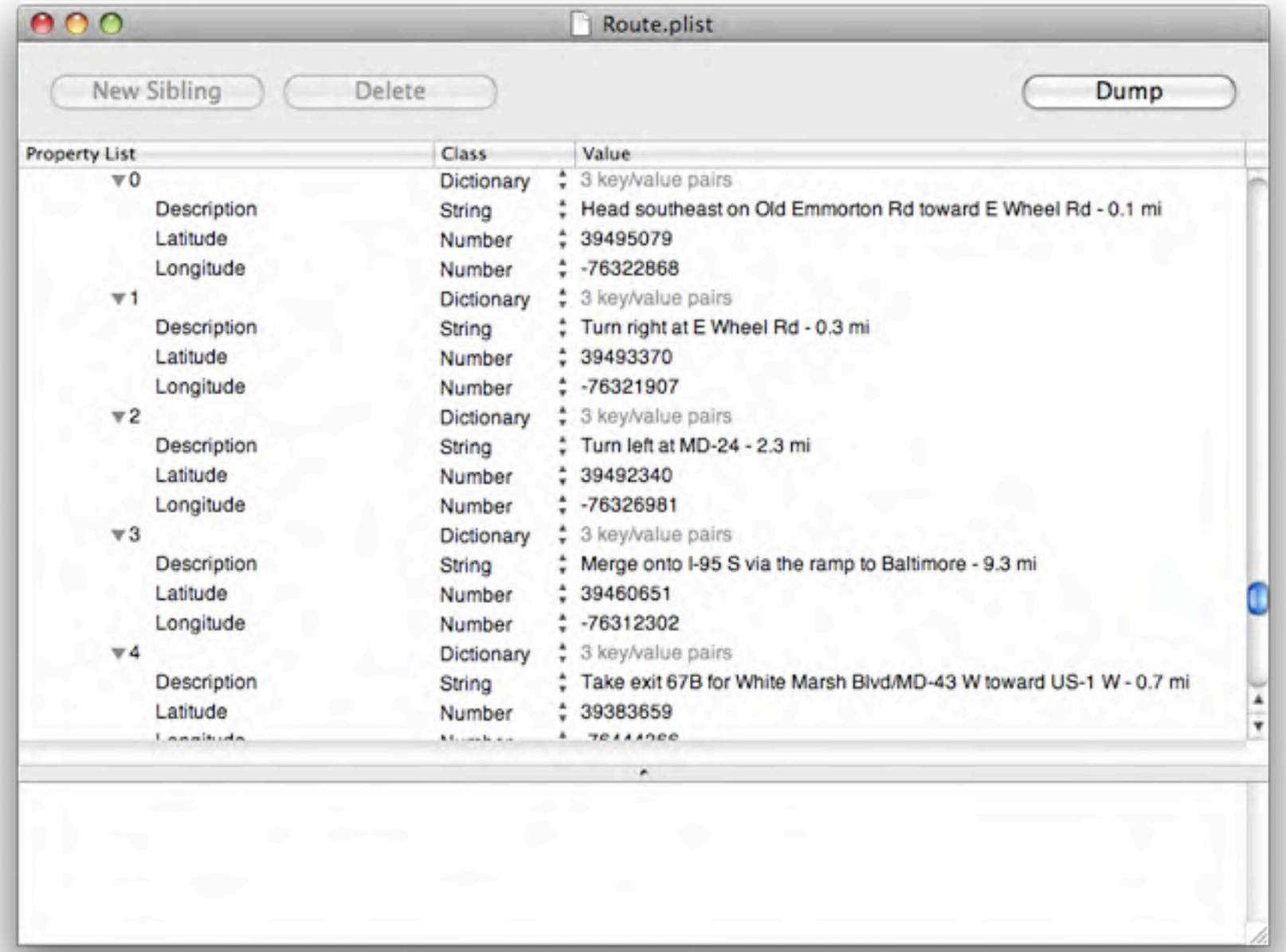
SQLite DB Example - SMS



iPhone Processing

What Can be Recovered?

Plist Example - Google Map Directions



iPhone Processing

Security - SIM Lock

- A SIM Lock can easily be defeated by removing the SIM card from the top of the iPhone by inserting a small pin into the small hole next to the 3.5mm earphone jack

iPhone

Backing up A Password Protected iPhone

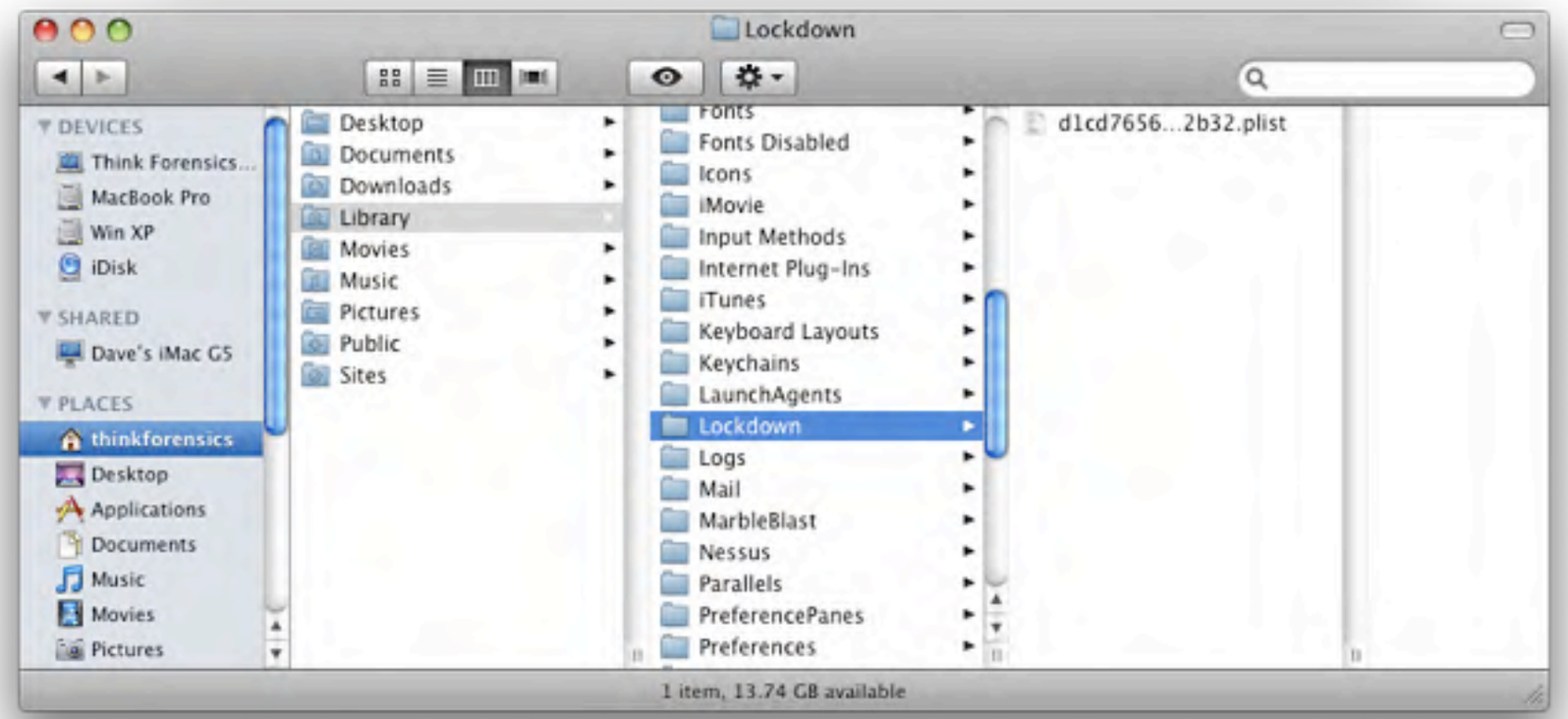
- When a phone is locked with a password, it can not be backed up to a user account other than its own
- A pairing file in the Lockdown folder located in the user's Library folder must be present
- Without the password to unlock the phone, it can't be backed up or synced to a forensic computer
- iPhone can be set to erase all data when 10 incorrect passcode attempts are made

iPhone

Backing up A Password Protected iPhone

- By copying the Lockdown folder located in the suspect user account's Library folder to a clean user account on a forensic Mac, the phone and be synced and backed up

- This will allow the examiner to view
  - Address book entries
  - Photos
  - Videos
- The iPhone can also now be backed up and the back up files can be processed

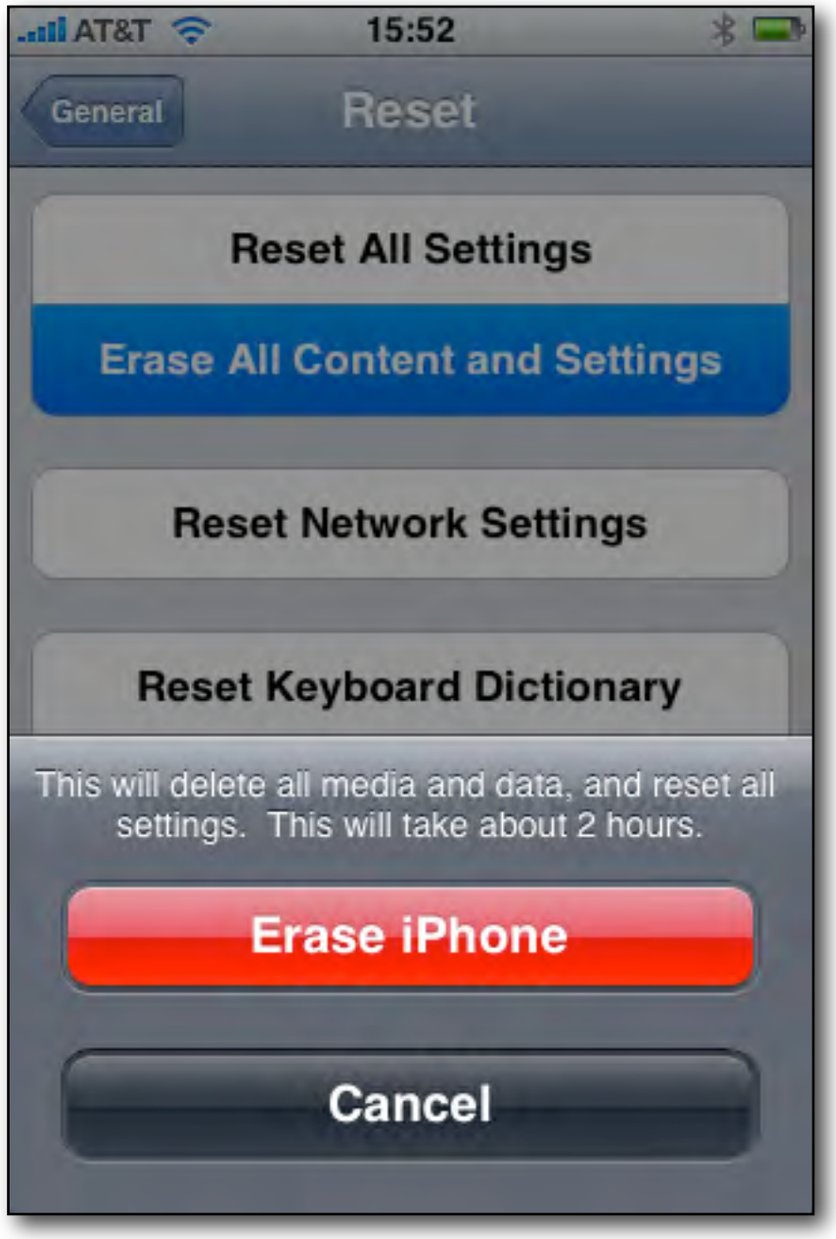


This is not a forensically sound process, dates and times will be changed.
The iPhone is not recognized if a hardware write block is placed between it and the Mac.

iPhone

Manually and Remotely Erasing iPhone

- A User of the iPhone with version 2.0 software can manually erase the iPhone
- The iPhone can also be erased remotely in an Enterprise environment
- An examiner may want to remove the SIM card if this is a concern



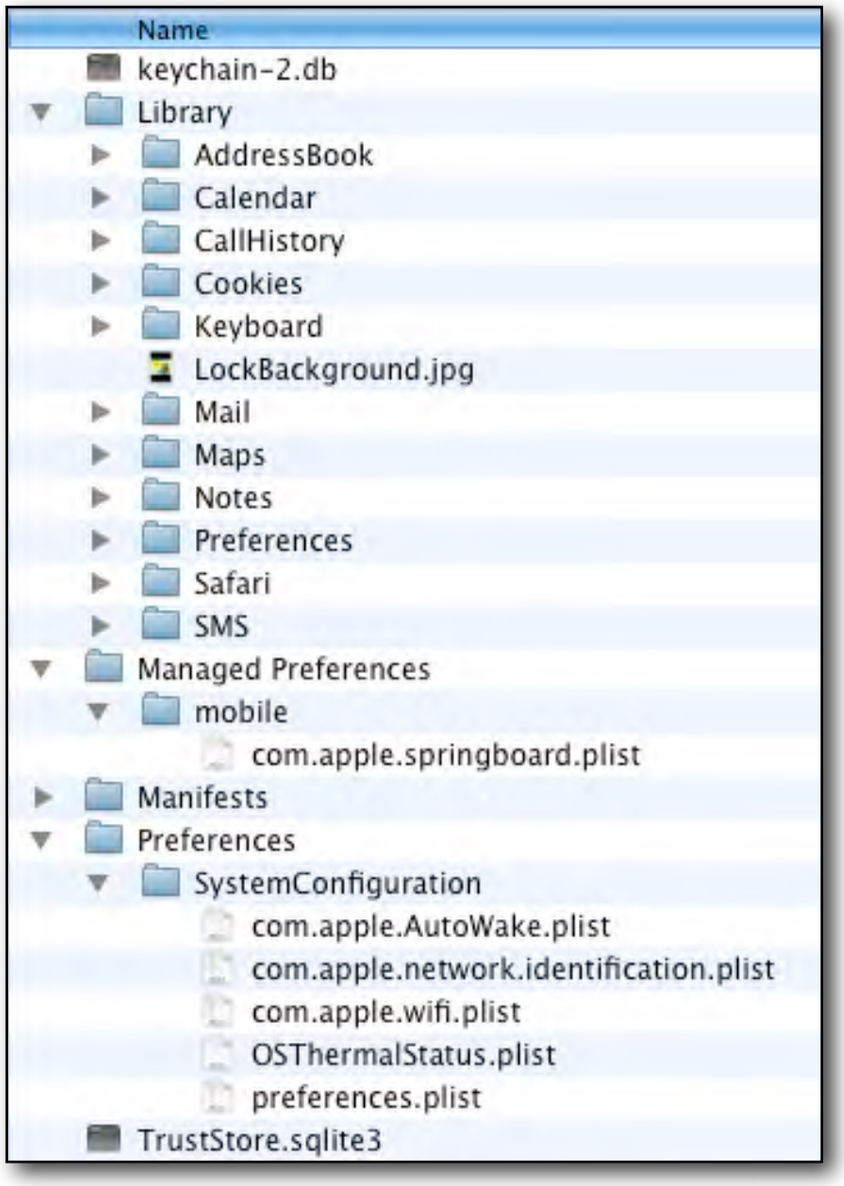
iPhone Processing

Cellebrite UFED

Cellebrite UFED is able to extract data from both locked and unlocked phones using the iPhone's backup service and other proprietary solutions.

Cellebrite UFED only sends data from the iPhone to a storage device which prevents any changes to the original system.

http://www.cellebrite.com/cellebrite-for-forensics-law-enforcement.html



Contact Information

Forward Discovery, Inc.

500 Montgomery Street
Suite 400
Alexandria, Virginia 22314
USA

Voice: +1 302.670.0015
Email: swhalen@forwarddiscovery.com
Skype: swhalen848