```
if (youWant(slides)) {
    Response->Redirect(S"http://www.dropbox.com/");
    enjoyComic();
} else {
    enjoyComic();
}
```

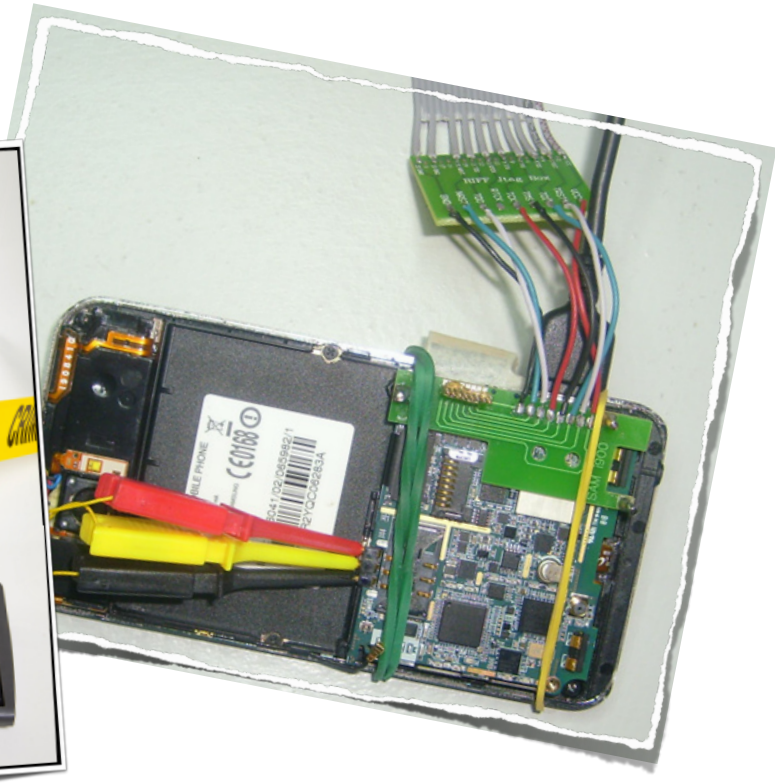
See also http://theoatmeal.com/comics/apple
(but not if you have sensitive eyes/ears)

Introduction to iPhone 4n6

Dan O'Day, d@4n68r.com
Purdue University
April 2, 2014

Introduction

Dan O'Day



Tentative Schedule

Time	Session Description
8:30am	iOS / iPhone Overview / DFU & Recovery Modes Lab
9:30am	Logical Acquisition
10:00am	Physical Acquisition (lecture only, no time for lab)
10:15am	Application / Data Analysis Lab

All labs are tentative and depend on device availability and time taken to acquire data

Preparation

- Go to http://supercrazyawesome.com/ and download iPhone Backup Extractor
- Go to http://www.iclarified.com —> Jailbreak Wizard —> Select Device —> Download jailbreak tool (evasi0n/redsn0w/etc.) if available and relevant IPSW firmware file
- Download a SQLite Browser (I recommend the 'SQLite Manager' Firefox Add-on)
- Begin backing up iDevice using iTunes

Preparation

Backups

Automatically Back Up

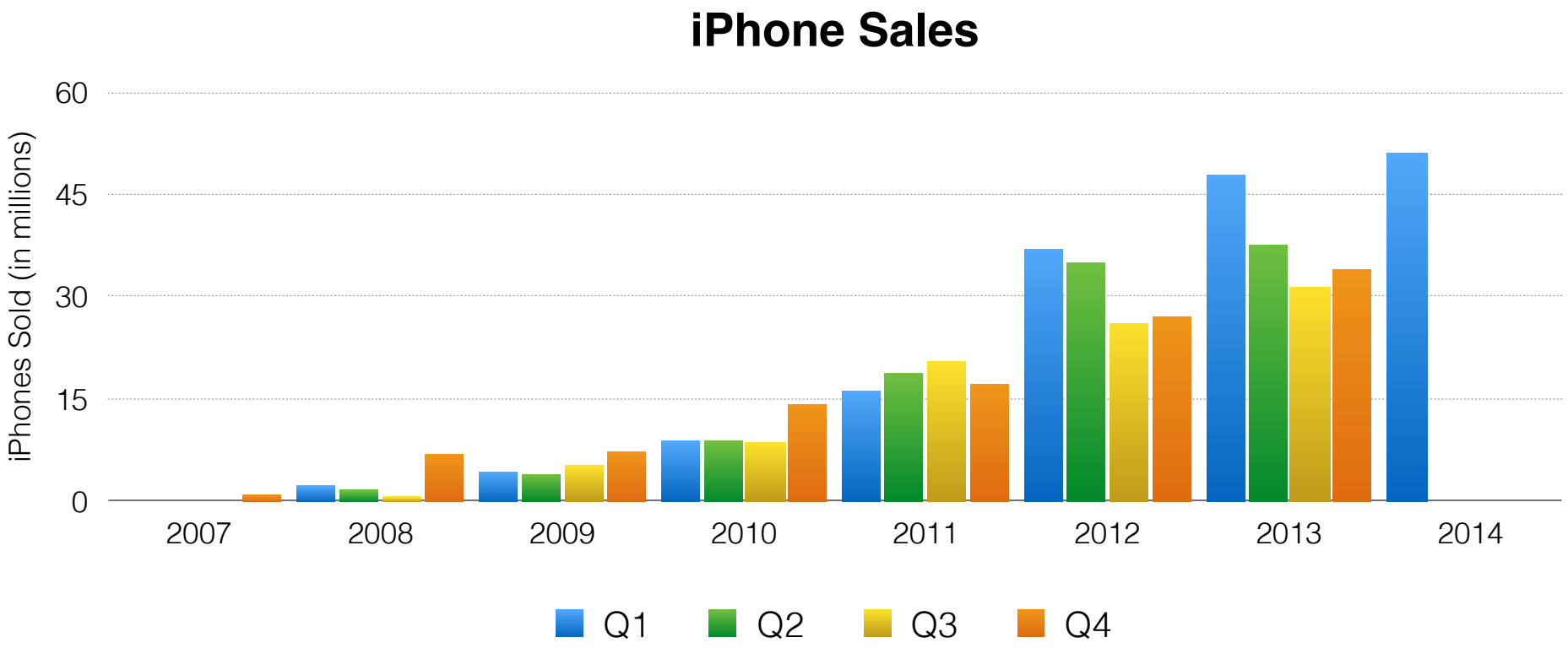
- iCloud
  Back up the most important data on your iPhone to iCloud.
- This computer
  A full backup of your iPhone will be stored on this computer.
  - Encrypt iPhone backup **NO!!!**
    This will also back up account passwords used on this iPhone.
    Change Password...

Manually Back Up and Restore

Manually back up your iPhone to this computer or restore a backup stored on this computer.

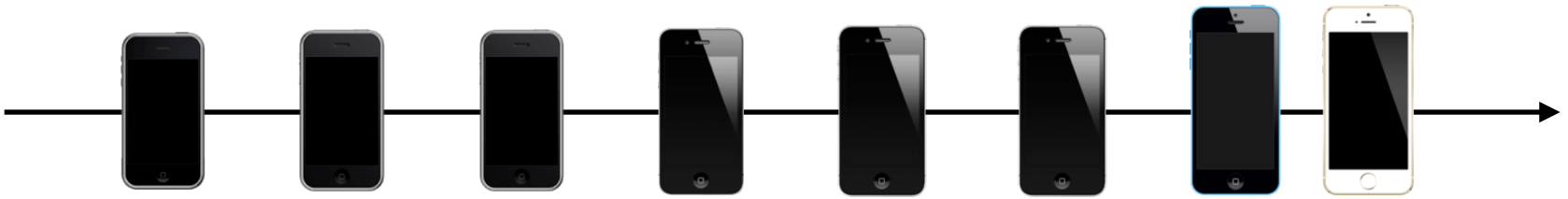
Back Up Now | Restore Backup...

Latest Backup:
Today 9:53 PM to this computer



Data retrieved from http://commons.wikimedia.org/wiki/File:IPhone_sales_per_quarter_simple.svg

iPhone Timeline



Jun 2007 | Jul 2008 | Jun 2009 | Jun 2010 | Oct 2011 | Sep 2012 | Sep 2013

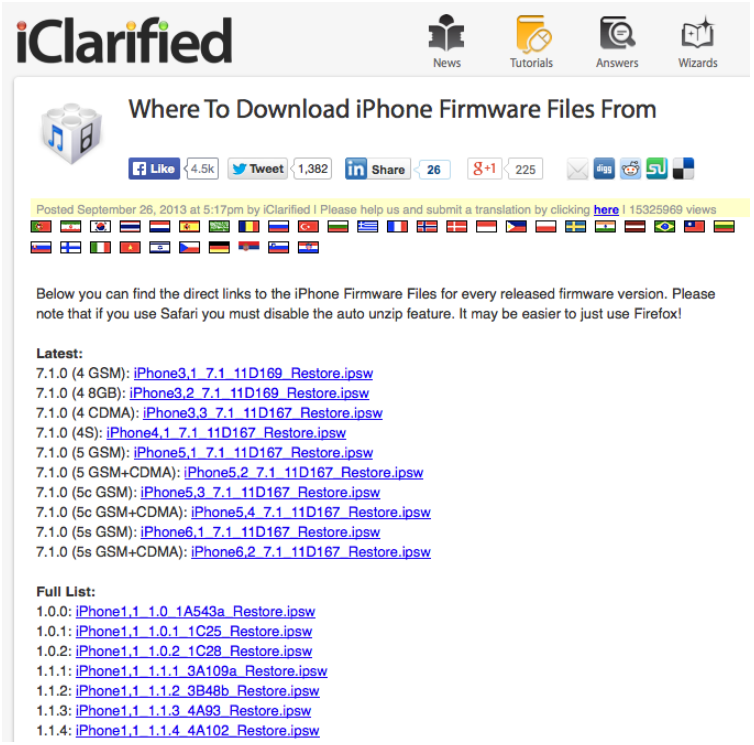
Which is Which?

- Model numbers (cf. http://support.apple.com/kb/ht3939)
- Siri only present in > 4s (depress home button)
- Visual comparison (5's are bigger)

Major iOS Releases

Date	iPhone OS / iOS Version
Jun 2007	1.0
Jul 2008	2.0
Jun 2009	3.0
Feb 2010	3.1.3
Jun 2010	4.0 (first iOS)
Nov 2010	4.2.1
Oct 2011	5.0
May 2010	5.1.1
Sep 2010	6.0
Feb 2014	6.1.6
Sep 2013	7.0
Mar 2014	7.1

iOS Firmware Files



iClarified

News Tutorials Answers Wizards

Where To Download iPhone Firmware Files From

Like 4.5k Tweet 1,382 Share 26 +1 225

Posted September 26, 2013 at 5:17pm by iClarified | Please help us and submit a translation by clicking here | 15325969 views

Below you can find the direct links to the iPhone Firmware Files for every released firmware version. Please note that if you use Safari you must disable the auto unzip feature. It may be easier to just use Firefox!

Latest:

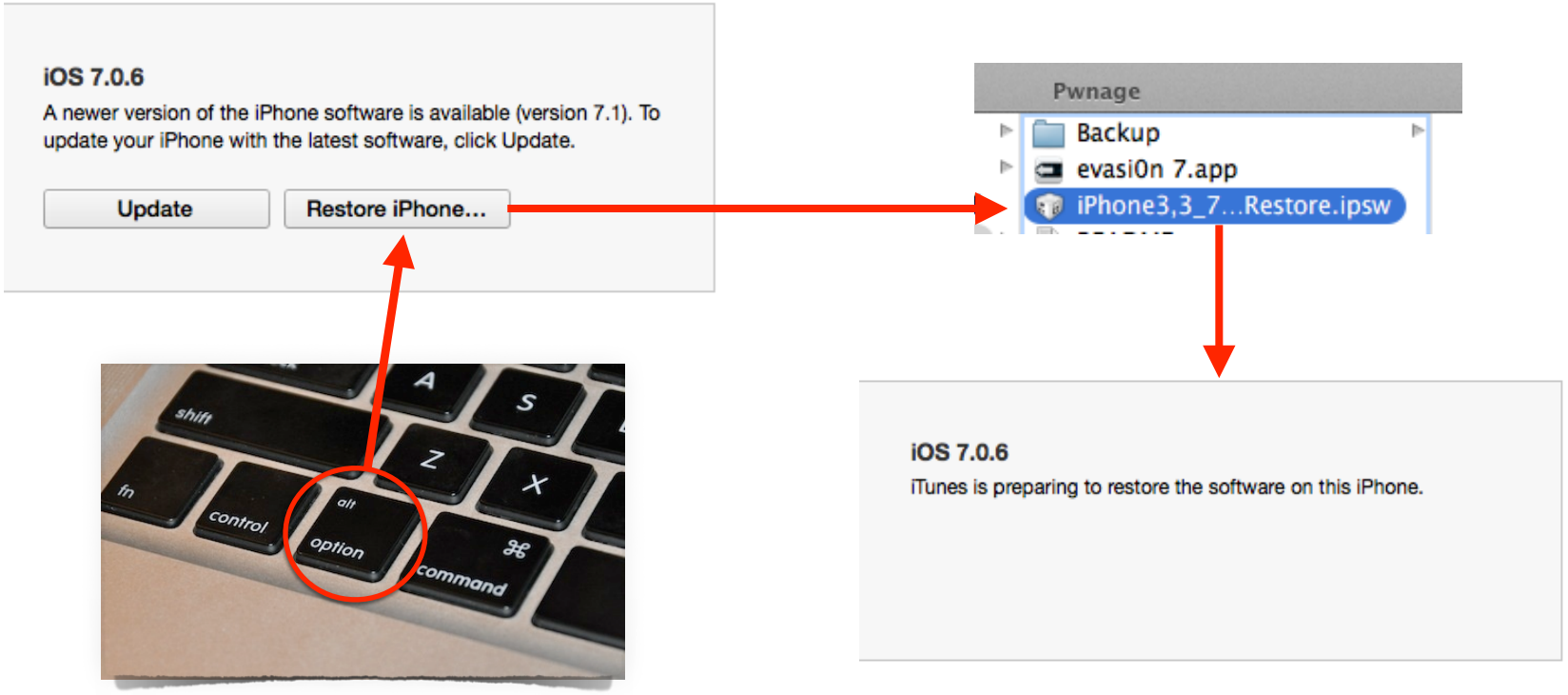
7.1.0 (4 GSM): iPhone3,1_7.1_11D169_Restore.ipsw
7.1.0 (4 8GB): iPhone3,2_7.1_11D169_Restore.ipsw
7.1.0 (4 CDMA): iPhone3,3_7.1_11D167_Restore.ipsw
7.1.0 (4S): iPhone4,1_7.1_11D167_Restore.ipsw
7.1.0 (5 GSM): iPhone5,1_7.1_11D167_Restore.ipsw
7.1.0 (5 GSM+CDMA): iPhone5,2_7.1_11D167_Restore.ipsw
7.1.0 (5c GSM): iPhone5,3_7.1_11D167_Restore.ipsw
7.1.0 (5c GSM+CDMA): iPhone5,4_7.1_11D167_Restore.ipsw
7.1.0 (5s GSM): iPhone6,1_7.1_11D167_Restore.ipsw
7.1.0 (5s GSM+CDMA): iPhone6,2_7.1_11D167_Restore.ipsw

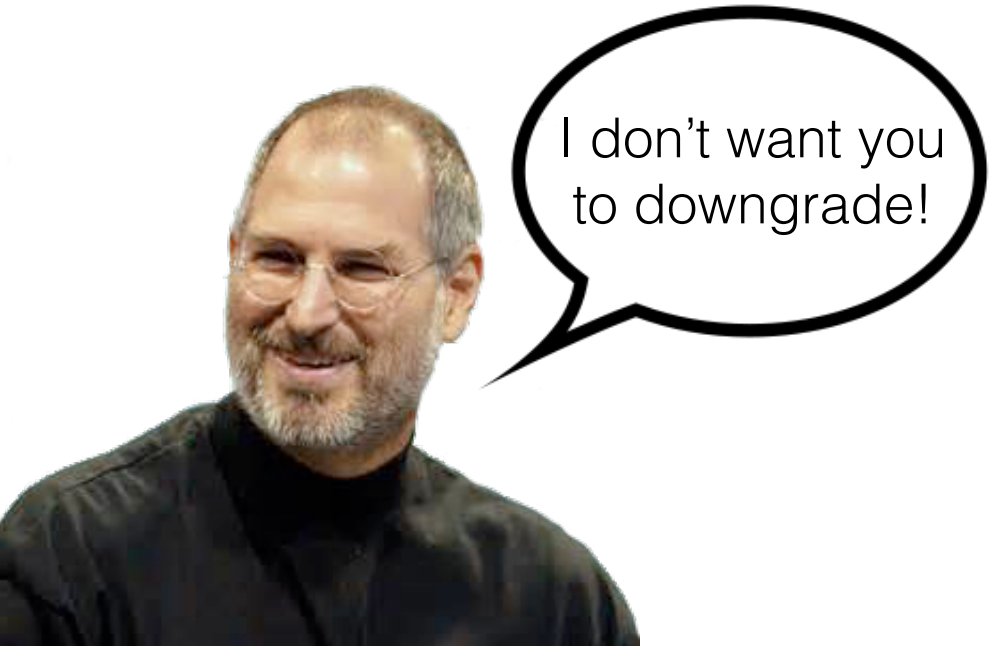
Full List:

1.0.0: iPhone1,1_1.0_1A543a_Restore.ipsw
1.0.1: iPhone1,1_1.0.1_1C25_Restore.ipsw
1.0.2: iPhone1,1_1.0.2_1C28_Restore.ipsw
1.1.1: iPhone1,1_1.1.1_3A109a_Restore.ipsw
1.1.2: iPhone1,1_1.1.2_3B48b_Restore.ipsw
1.1.3: iPhone1,1_1.1.3_4A93_Restore.ipsw
1.1.4: iPhone1,1_1.1.4_4A102_Restore.ipsw

http://www.iclarified.com/entry/index.php?enid=750

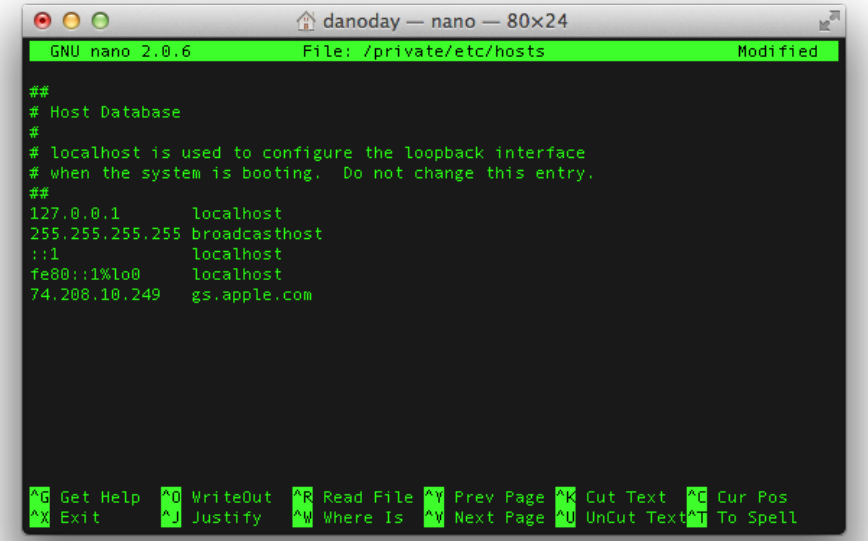
Restore Device to Specific IPSW





Workaround

```
T0huWav0hu:~ danoday$ sudo nano /private/etc/hosts
```



Data Storage (Physical)

- All data stored on internal NAND flash
  - NAND review:
    - Limited P/E cycles, page must be erased by writing all 1's
    - Wear leveling applies, but thanks to encryption, file carving is often a waste of time

Disk Partitions

- /dev/rdisk0 = entire disk
  - /dev/rdisk0s1 (Slice 1) = firmware partition (IPSW)
  - /dev/rdisk0s2 (Slice 2) = user data partition (what we want)

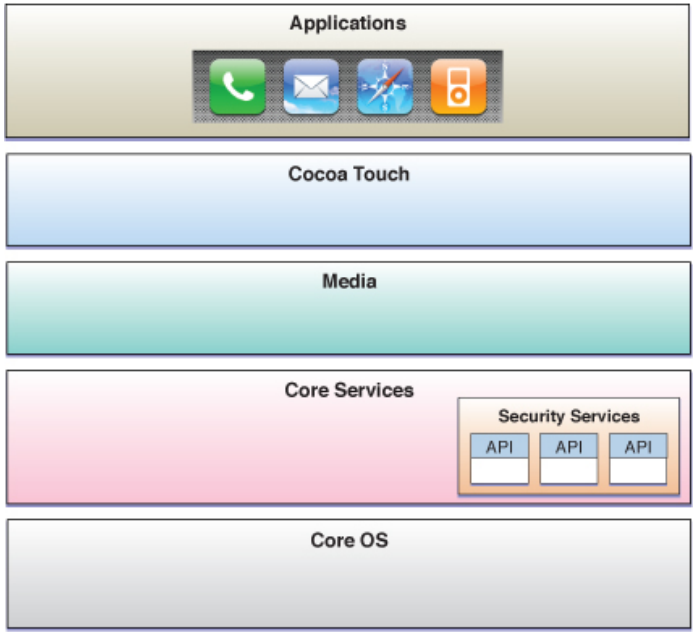
iPhone Encryption SUCKS FOR 4n68rs

- iOS 4 introduced hardware encryption
- iOS 3 (3GS): device-level
- iOS 4/5: File System Key (encrypts entire file system) AND Class Key (separate encryption for each file)
- iOS 6: dedicated AES-256 key/crypto engine for each device (hardware layer), kernel / memory ASLR (between flash storage and main system memory) + data protection w/passcode (software layer, apps must opt-in and ensure data not shared)
- iOS 7: data protection on by default (full encryption at hardware *and* software layers), but still requires passcode

What does this mean for 4n68rs?

On the Bright Side…

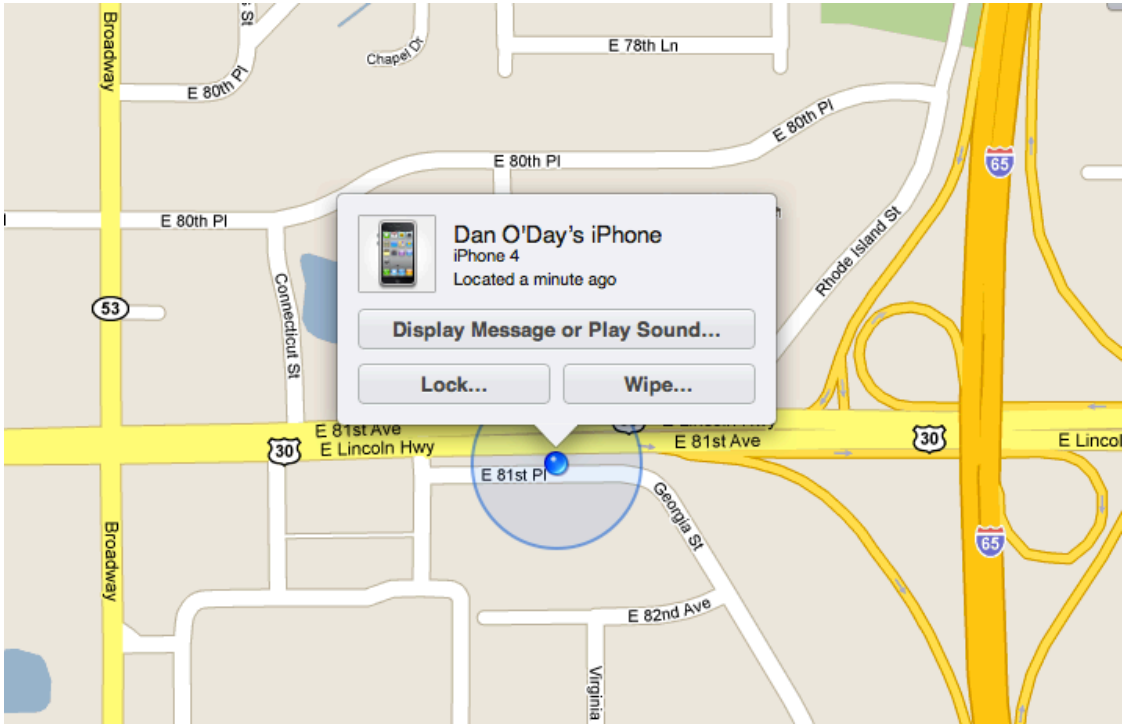
- File system is mostly unlocked once device is booted up
- Baseline encryption is NOT tied to passcode/PIN
  - Data protection is, however - but only if passcode/PIN enabled!



- **Core OS** (BSD & Mach = Darwin w/XNU kernel)
- **Core Services** (system & security services used by apps)
- **Cocoa Touch** (GUI / UX)
- **Applications**

iPhone Seizure

- Isolate device from network!!!



iPhone Seizure

- If possible, attempt to gain access in RF-blocked environment
  - Oh wait, that doesn't work…. (cf. https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2010-27.pdf)
  - Airplane mode if able (i.e. no passcode/PIN)

CERIAS Tech Report 2010-27
A Field Test of Mobile Phone Shielding Devices
by Eric Katz
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

If the device is wiped, is the data really gone?

- YES!!!
  - Writes all 1's to flash media then reinstalls OS
  - Backup files on user's computer
  - However, many apps store the device UUID on a remote server

Accessing iPhone Data (hacking iOS)

- Jailbreaking = replacing Apple firmware (slice 1) with custom (hacked) firmware
  - Can be used to allow physical acquisition of iPhone 4 or less (i.e. NOT helpful in bypassing data encryption in iPhone 4s, 5, 5c, or 5s)

Jailbreaking Legality

- iPhone… go for it!
- iPad… STOP immediately! (cf. http://s3.amazonaws.com/public-inspection.federalregister.gov/2012-26308.pdf)
  - DCMA law as of October 28, 2012
  - Exemption from 1998 Digital Millennium Copyright Act (DMCA) made for smartphones
  - Only exception for tablets is to enable access via assistive technology

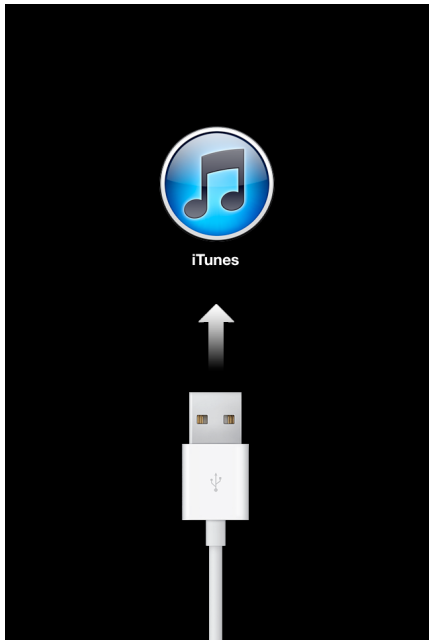
Jailbreaking Tools

redsn0w 0.9.15 beta 3[109][110]	November 1, 2012	iPhone 3GS · iPhone 4 · iPod Touch · iPad [71][109][111]	4.1–6.1.6
Absinthe 2.0.4[90]	May 30, 2012	iPhone 3GS · iPhone 4 · iPhone 4S · iPod Touch · iPad · iPad 2 · iPad (3rd generation) [91]	5.1.1[91]
evasi0n	February 4, 2013	iPhone 3GS · iPhone 4 · iPhone 4S · iPhone 5 · iPod Touch (4th generation) · iPod Touch (5th generation) · iPad 2 · iPad 4 · iPad (3rd generation) · iPad mini	6.0-6.1.2[114]
evasi0n7	December 22, 2013	iPhone 4 · iPhone 4S · iPhone 5 · iPhone 5S · iPhone 5C · iPod Touch (5th generation) · iPad 2 (fixed 1.0.2 beta) · iPad 4 · iPad (3rd generation) · iPad Air · iPad mini · iPad mini (2nd generation)	7.0-7.0.6[114]
p0sixspwn	December 30, 2013	iPhone 3GS · iPhone 4 · iPhone 4S · iPhone 5 · iPod Touch (4th generation) · iPod Touch (5th generation) · iPad 2 · iPad (3rd generation) · iPad 4 · iPad mini	6.1.3-6.1.6 (6.1.6 via redsn0w + p0sixspwn Cydia package only.)

Retrieved from http://en.wikipedia.org/wiki/IOS_jailbreaking

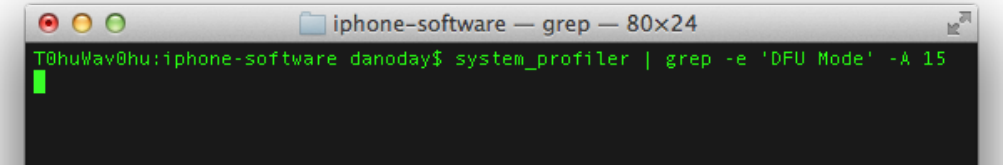
Recovery & DFU Modes

- To perform certain functions, must place device in device failsafe utility (DFU) or recovery mode
- Bypasses loading of OS
- DFU mode = black screen
- Recovery mode =



Verify DFU Mode

- DFU mode = black screen
  - Connect device and ensure powered off
  - Hold down Power + Home for about 10 seconds
  - Release Power, but continue holding Home for about 10 more seconds
  - Release Home button (screen should now be black)
  - Mac Terminal command:



Recovery Mode

- Recovery mode
  - Power off device
  - Hold down Home button and plug in while holding

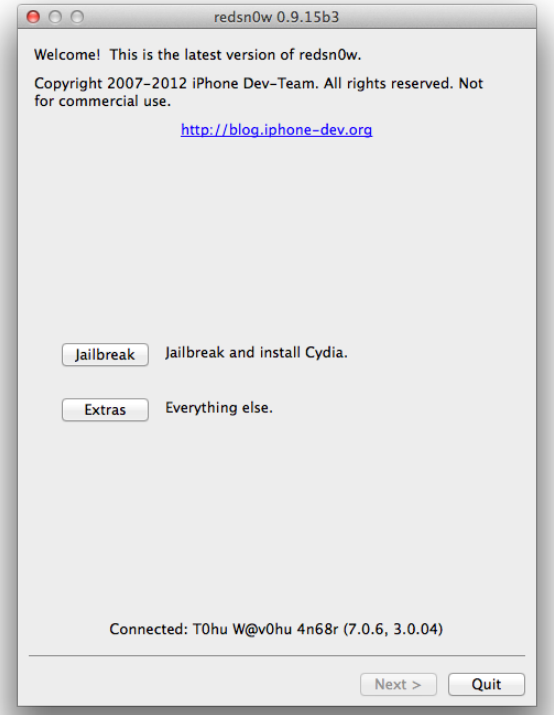
Exit Recovery/DFU Mode

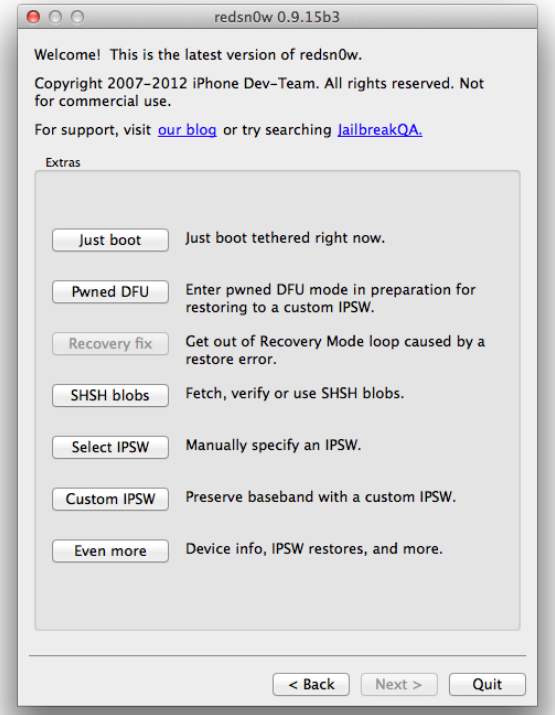
- Hold Power + Home till you see Apple logo (reboot)
  - What if stuck in recovery loop?
    - Use iRecovery (cf. http://theiphonewiki.com/wiki/IRecovery & https://github.com/iH8sn0w/irecovery)

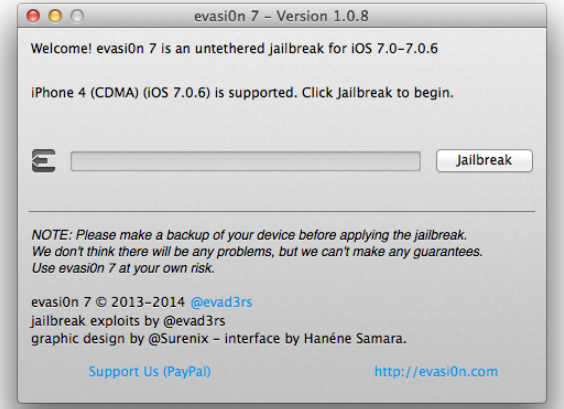
```
./irecovery -s

setenv auto-boot true

/exit
```

    - Reboot device

Jailbreak Examples (redsn0w & evasi0n/7)







Logical Acquisition Lab

Preparation

Backups

Automatically Back Up

- iCloud
  Back up the most important data on your iPhone to iCloud.
- This computer
  A full backup of your iPhone will be stored on this computer.
  - Encrypt iPhone backup **NO!!!**
    This will also back up account passwords used on this iPhone.
    Change Password...

Manually Back Up and Restore

Manually back up your iPhone to this computer or restore a backup stored on this computer.

Back Up Now | Restore Backup...

Latest Backup:
Today 9:53 PM to this computer

Preparation

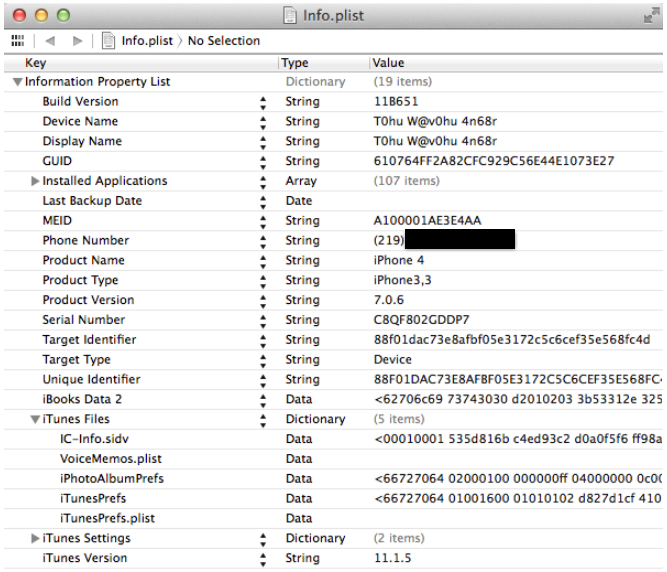
- Go to http://supercrazyawesome.com/ and download iPhone Backup Extractor
- Go to http://www.iclarified.com —> Jailbreak Wizard —> Select Device —> Download jailbreak tool (evasi0n/redsn0w/etc.) if available and relevant IPSW firmware file
- Download a SQLite Browser (I recommend the 'SQLite Manager' Firefox Add-on)
- Begin backing up iDevice using iTunes

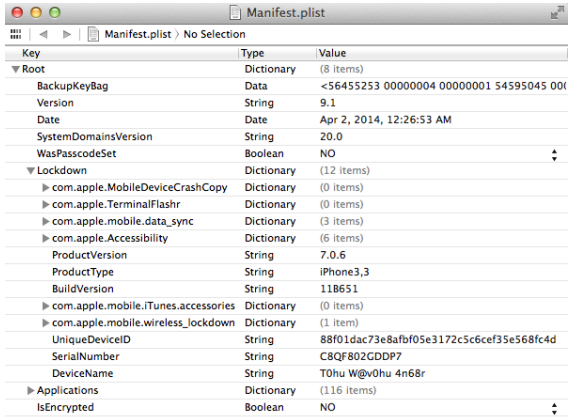
Logical Acquisitions

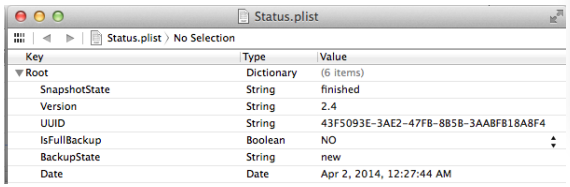
1. Backup Acquisition (iTunes + F/OSS)
2. Proprietary Logical (COTS)

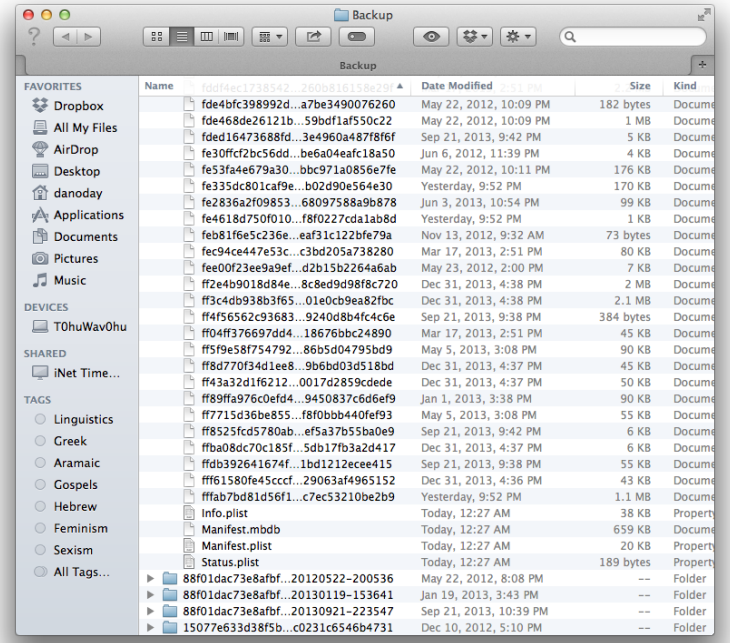
iTunes Backup

- Location:
  ~/Library/Application Support/MobileSync

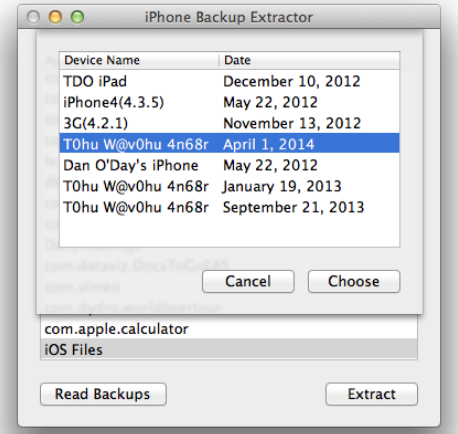


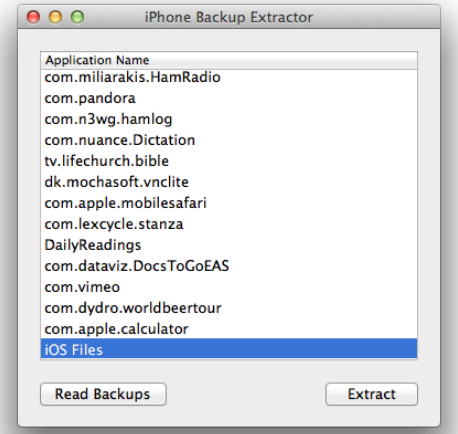






iPhone Backup Extractor





What if the backup is encrypted?

Elcomsoft Phone Password Breaker

Like 511 people like this. Sign Up to see what your friends like.

Recover Password-Protected BlackBerry and Apple Backups

Elcomsoft Phone Password Breaker enables forensic access to password-protected backups for smartphones and portable devices based on RIM BlackBerry and Apple iOS platforms. The password recovery tool supports all Blackberry smartphones as well as Apple devices running iOS including iPhone, iPad and iPod Touch devices of all generations released to date, including the iPhone 5S and iOS 7.

Unlock Apple and BlackBerry Backups

The new tool recovers the original plain-text passwords protecting encrypted backups for Apple and BlackBerry devices. The backups contain address books, call logs, SMS archives, calendars and other organizer data, camera snapshots, voice mail and email account settings, applications, Web browsing history and cache.

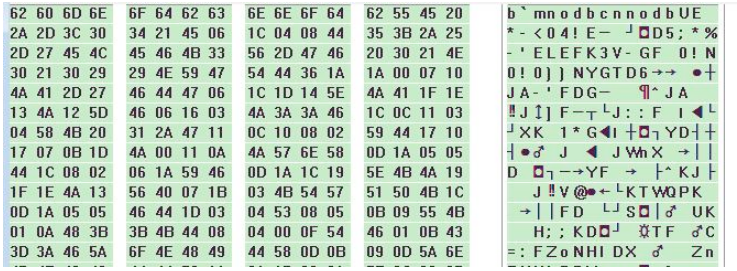
Recover online backups from Apple iCloud

(Good luck)

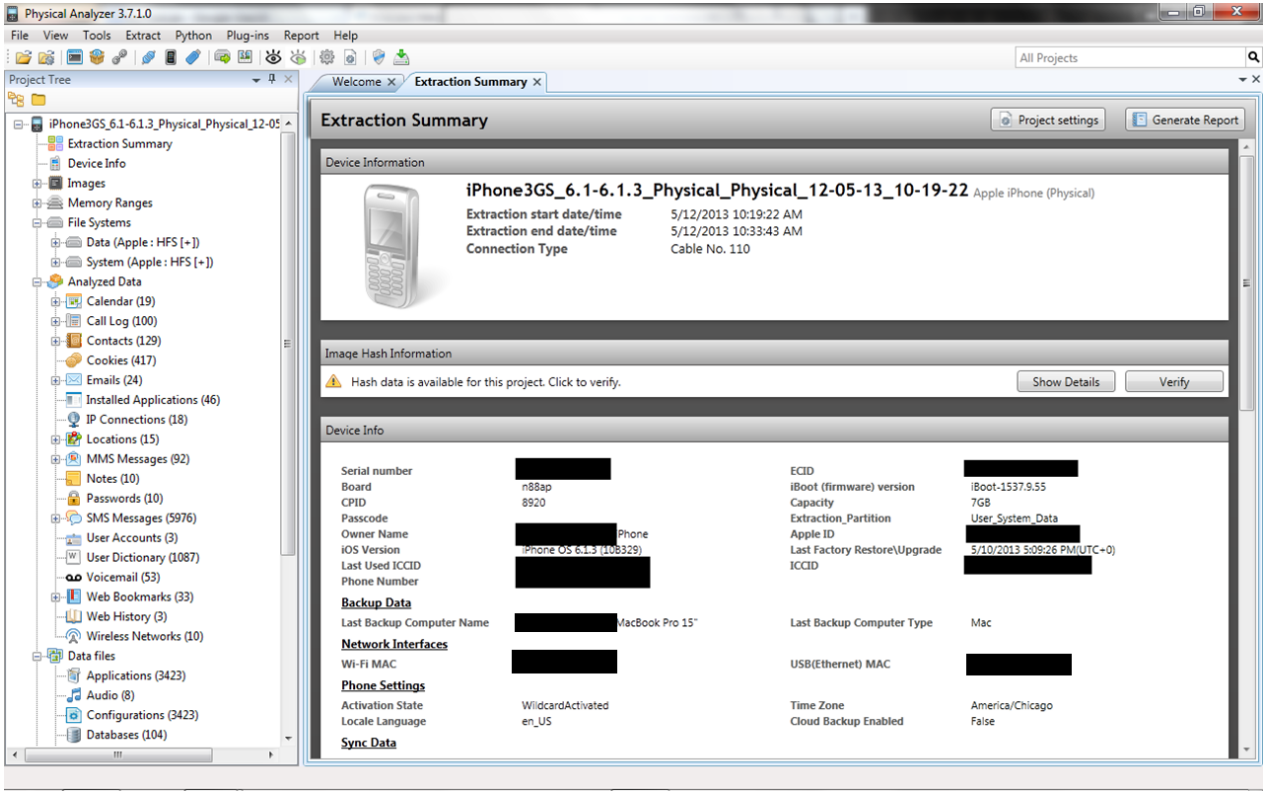
Encrypted Backup

- If backup is NOT encrypted, keychain will be
- If backup IS encrypted, the keychain will be in plaintext *if* you crack the backup password

Physical Acquisition



Proprietary Acquisition - Cellebrite



Cellebrite

Device	Physical extraction	Physical extraction with password bypass	Physical extraction decoding	File system extraction*	Logical extraction*
iPhone 2G	✓	✓	✓	✓	✓
iPhone 3G	✓	✓	✓	✓	✓
iPhone 3GS	✓	✓	✓	✓	✓
iPhone 4	✓	✓	✓	✓	✓
iPhone 4S				✓	✓
iPhone 5				✓	✓
iPod Touch 1G	✓	✓	✓	✓	✓
iPod Touch 2G	✓	✓	✓	✓	✓
iPod Touch 3G	✓	✓	✓	✓	✓
iPod Touch 4G	✓	✓	✓	✓	✓
iPod Touch 5G				✓	✓
iPad Mini				✓	✓
iPad 1	✓	✓	✓	✓	✓
iPad 2				✓	✓
iPad3				✓	✓
iPad 4				✓	✓

*Logical and File System extractions are only possible when the devices are unlocked.

VIAFORENSICS

iOS COMING SOON

viaExtract will soon support iOS physical, iOS logical, and Android physical acquisitions.

Elcomsoft

	iPhone 3G iPod Touch 1/2		iPhone 3Gs, iPod Touch 3th gen, iPad 1		iPhone 4 iPod Touch 4th gen iPod Touch 5th gen (***) iPad 2+, iPad Mini (***) iPhone 4S/5 (***)
	iOS 1..3	iOS 4.x	iOS 3	iOS 4/5	iOS 4/5/6/7
Physical imaging	✓	✓	✓	✓	✓
Logical imaging	✓	✓	✓	✓	✓
Passcode recovery	instant	✓	instant	✓	✓
Keychain decryption	✓	✓	✓	✓	✓
Disk decryption(*)	N/A*	N/A**	N/A*	✓**	✓

Physical acquisition of last-generation iOS 7 devices is possible if either of the following is true:

- There is no passcode protection on the device, or
- The investigator knows the passcode, or
- The device is jailbroken

Other Proprietary/Restricted Methods

- Zdiarski method (free to law enforcement, requires command line fu)
- Elcomsoft
- Lantern (Katana Forensics)
- iXAM
- AccessData's MPE/+

Jailbreak Physical Acquisition

- WARNING: requires modifying slice 1 (jailbreaking) as well as installing software in and using slice 2 (enabling ssh)
- DOES NOT WORK for devices using hardware encryption of slice 2 (iPhone 4s and greater)
- `ssh root@192.168.1.1 dd if=/dev/rdisk0 bs=1M | dd of=ios-image.dmg`
- Default root pasword is ‘alpine’
- Other methods also feasible (push netcat, capture dd output through listening port, basic network hacking skills apply, etc.)

Physical Acquisition With FREE GUI Tool

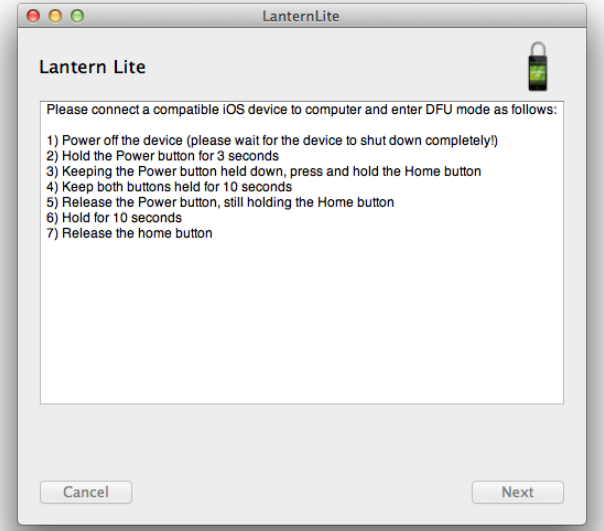
- Must have redsn0w and relevant IPSW on desktop (and *only* relevant IPSW file)

LANTERN Imager

Lantern Imager is another **free** product created by Katana Forensics. It is the first GUI based imaging product for Macintosh computers. Lantern Imager images all external media. Lantern Imager also has a built in write blocker within the application. The following media can be imaged utilizing Lantern Imager:

- Mac computers in FireWire/Thunderbolt Disk Mode
- Any Hard Drive
- Any USB Thumb Drive
- Any External USB Drive
- Any SD Cards including those from Android cell phones and GoPro's

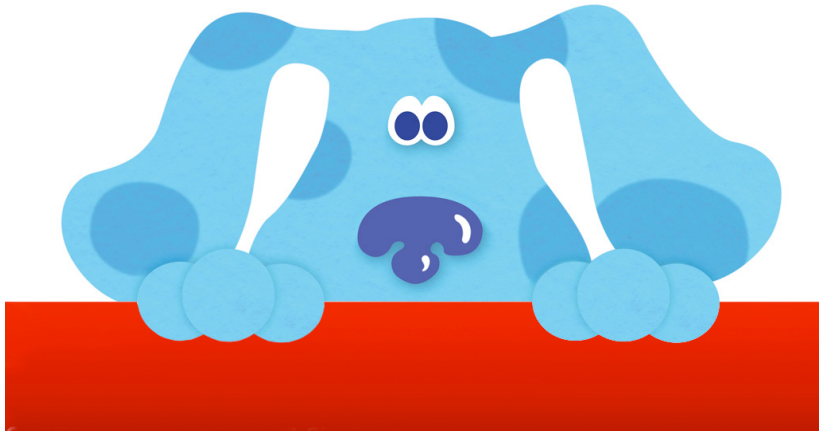
DOWNLOAD FROM CUSTOMER PORTAL



Lantern Lite Method

- Lantern Lite modifies the IPSW on the desktop to create a custom virtual RAM disk for slice 1 of the iOS device
- redsn0w loads this virtual slice into memory to gain access to the user slice, never actually modifying the original slice 1 on the device (nor slice 2 for that matter)
- Decrypts passcode on iPhone 4 and below (brute force, slow)
- Acquires raw physical image of user partition (assuming passcode is cracked)
- Decrypts user partition when finished, hashes image (SHA1) and creates log file

Application / Data Analysis



Main File Types Found on iPhones

- Property lists (plists)
  - Key/value pairs (serialized objects) in XML format (can be ASCII or binary, i.e. bplist)
- SQLite databases
- Keychains
  - Username and password information
  - Encrypted (AES 256-bit)

Places to Look (General)

- Backup (iOS Files)/SystemConfiguration/preferences.plist
- Backup/keychain-backup.plist (must be decrypted)
  (cf. https://github.com/ptoomey3/Keychain-Dumper)
- Backup/Media
- Backup/Library

Helpful SQL Commands

- SELECT * FROM table;
- SELECT column1, column2 FROM table WHERE column1 > 1
- SELECT datetime([date], ‘unixepoch’, ‘localtime’) as timestamp FROM table
  - Are the timestamps off? Unix epoch = seconds since 1/1/1970, but Apple uses 1/1/2001, so add 978307200 seconds to the Unix epoch. Example:
  - select datetime([date] + 978307200, 'unixepoch', 'localtime') as dt from message;