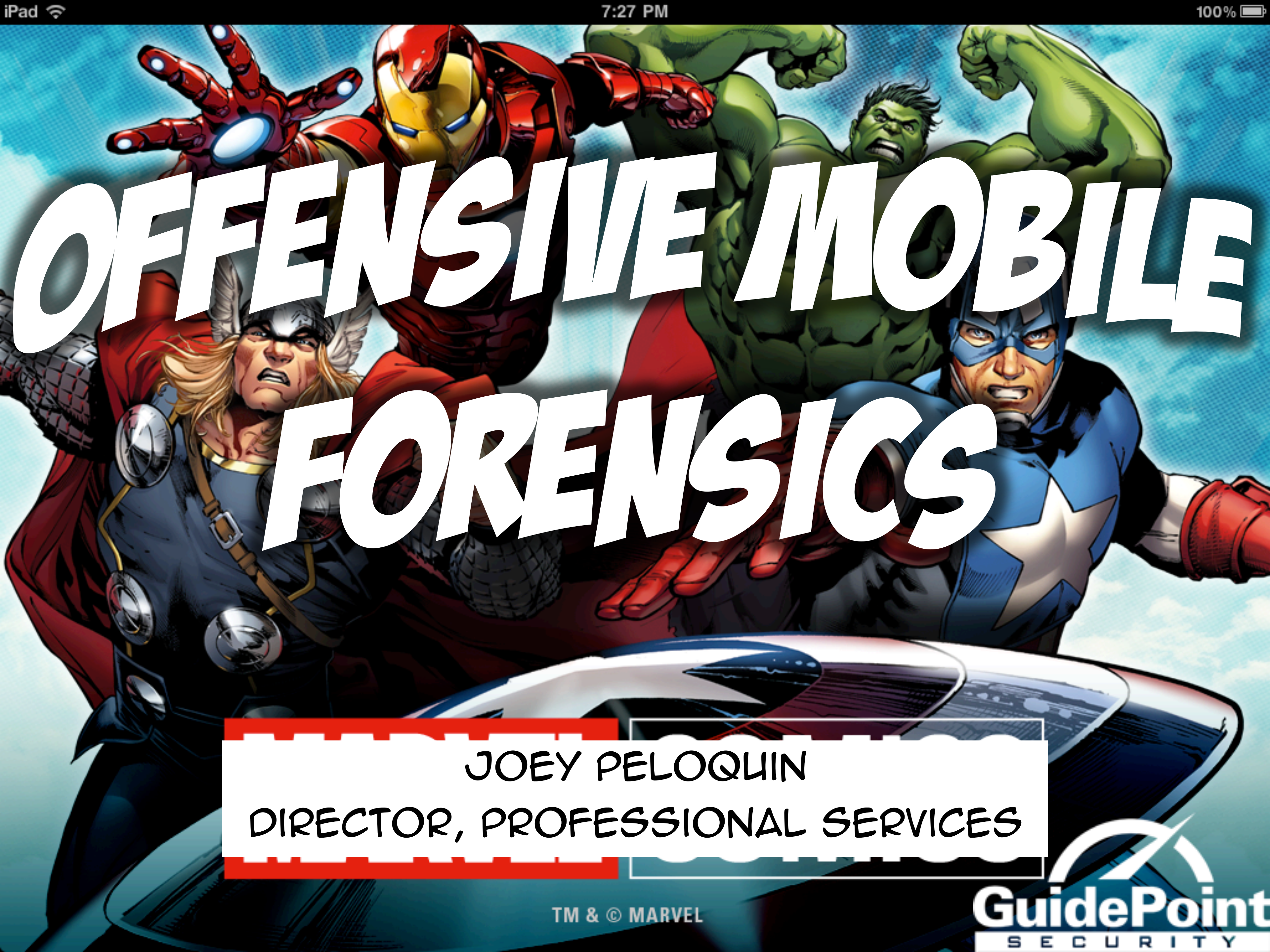


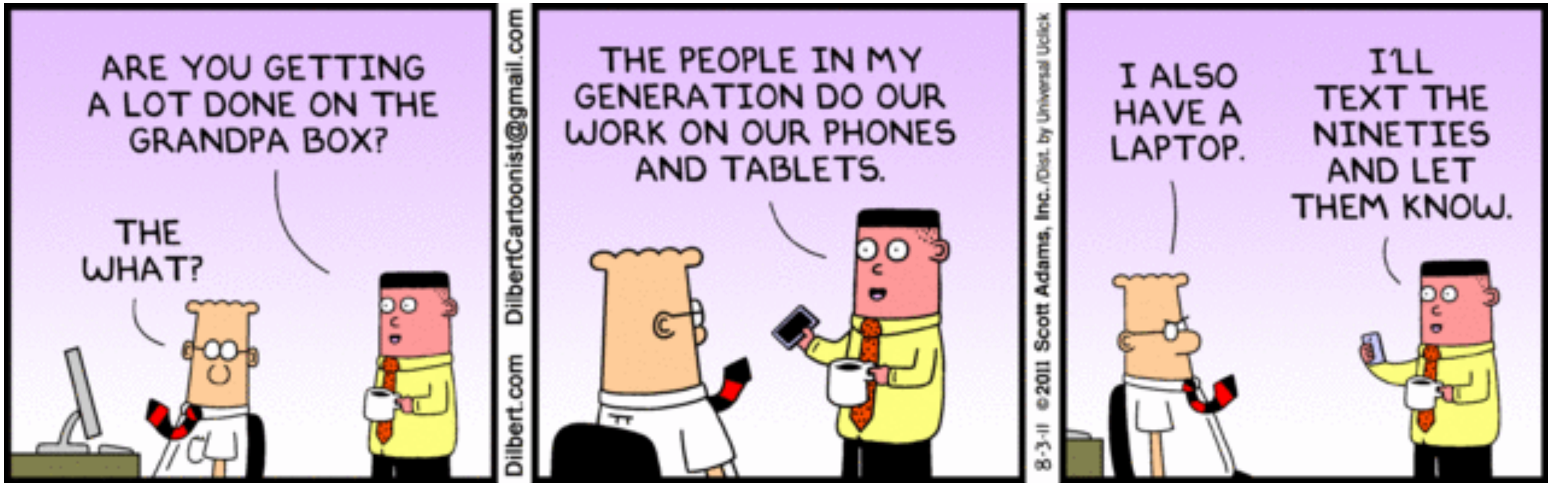
OFFENSIVE MOBILE FORENSICS

JOEY PELOQUIN
DIRECTOR, PROFESSIONAL SERVICES

GuidePoint
SECURITY

AGENDA

- INTRO
- TOOLS
- APPLE IOS
- GOOGLE ANDROID


ARE YOU GETTING A LOT DONE ON THE GRANDPA BOX?
THE WHAT?
THE PEOPLE IN MY GENERATION DO OUR WORK ON OUR PHONES AND TABLETS.
I ALSO HAVE A LAPTOP.
I'LL TEXT THE NINETIES AND LET THEM KNOW.

Dilbert.com DilbertCartoonist@gmail.com

8-3-11 ©2011 Scott Adams, Inc./Dist. by Universal Uclick

INTRODUCTION

BYOD
YOU'RE NOT THE ONLY ONE FEELING THE STRAIN OF MOBILE THREATS.
DIY.DESPAIR.COM

INTRODUCTION

- WHO AM I?
- MOBILE THREATS
- DEFINE:
  OFFENSIVE
  MOBILE
  FORENSICS
- TAKE-AWAYS
- QUESTIONS?

"There are a lot of security issues in the design of the iPhone that lend themselves to retaining more personal information than any other device."
– Jonathan Zdziarski

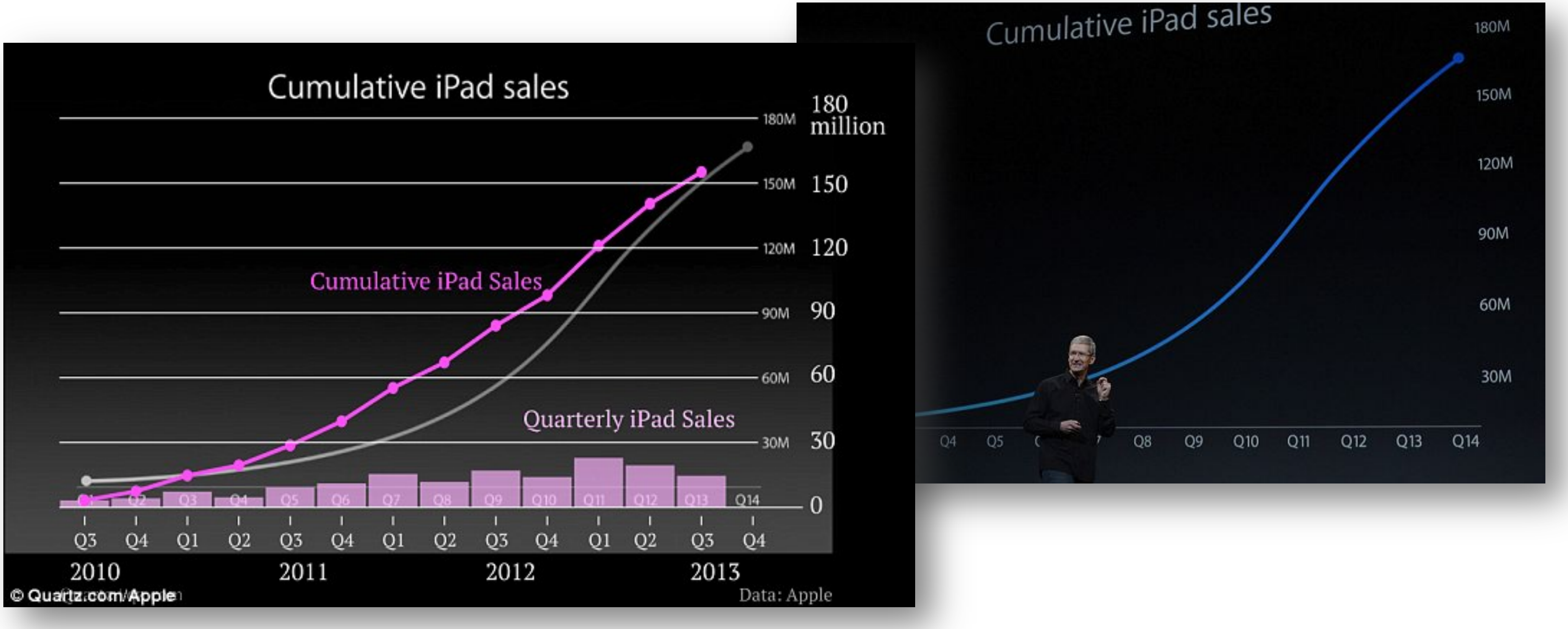
INTRODUCTION

- GOOGLE STATS
  - 400M+ DEVICES SOLD PER QTR
  - 15 SMARTPHONE MANUFACTURERS
  - 12 TABLET MANUFACTURERS
  - 51.8% MARKET SHARE (0913)

Version	Codename	Distribution
2.3.3 - 2.3.7	**Gingerbread**	**19%**
3.2	Honeycomb	0.1%
4.0.3 - 4.0.4	ICS	15.2%
4.1.x	**Jelly Bean**	**35.3%**
4.2.2		**17.1%**
4.3		**9.6%**
4.4	**KitKat**	**2.5%**

Introduction

- Apple Stats
  - 40.6% market share
  - 170M iPads sold
  - 9M 5S/C sold first weekend

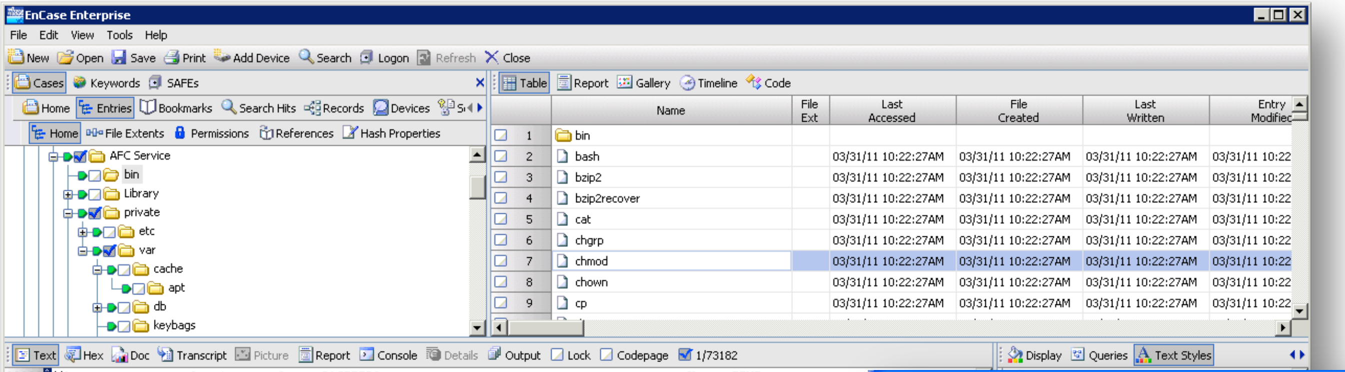


© Quartz.com/Apple

Data: Apple

TOOLS

TOOLS

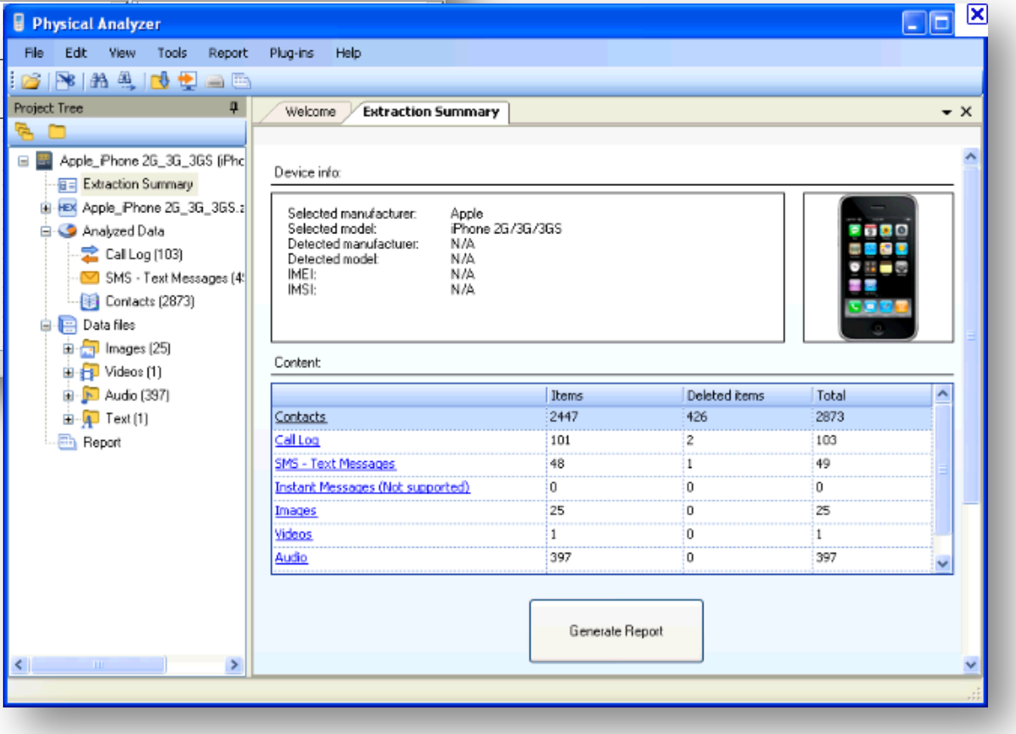


EnCase Enterprise

		Name	File Ext	Last Accessed	File Created	Last Written	Entry Modified
□	1	bin					
□	2	bash		03/31/11 10:22:27AM	03/31/11 10:22:27AM	03/31/11 10:22:27AM	03/31/11 10:22
□	3	bzip2		03/31/11 10:22:27AM	03/31/11 10:22:27AM	03/31/11 10:22:27AM	03/31/11 10:22
□	4	bzip2recover		03/31/11 10:22:27AM	03/31/11 10:22:27AM	03/31/11 10:22:27AM	03/31/11 10:22
□	5	cat		03/31/11 10:22:27AM	03/31/11 10:22:27AM	03/31/11 10:22:27AM	03/31/11 10:22
□	6	chgrp		03/31/11 10:22:27AM	03/31/11 10:22:27AM	03/31/11 10:22:27AM	03/31/11 10:22
□	7	chmod		03/31/11 10:22:27AM	03/31/11 10:22:27AM	03/31/11 10:22:27AM	03/31/11 10:22
□	8	chown		03/31/11 10:22:27AM	03/31/11 10:22:27AM	03/31/11 10:22:27AM	03/31/11 10:22
□	9	cp		03/31/11 10:22:27AM	03/31/11 10:22:27AM	03/31/11 10:22:27AM	03/31/11 10:22

```
00000Îúíþ··············0··|·······8···__PAGEZERO··························H···__TEXT·········
00120·0················__text·········__TEXT·························|·······__symbol_stub4··__TEXT··
00240···h·················|·········__cstring········__TEXT·········|$··e···|···················__const··
00360__TEXT·········ä3··|···ä#··························__DATA···········@·······0··············__nl_
00480ptr··__DATA··········@··D····0·················^·······__data·········__DATA········D@··@···DO·········
00600·····__dyld··········__DATA·········|@······|0····························__la_symbol_ptr··__DATA·········@··x··
00720···········o·········__const·········__DATA··········B··Ô····2························__bss·········__DATA··
00840iB···|·······························__common··········__DATA··········1D····························8···
00960IT·······P····0····@····$···························@··9···àQ··d········P········G····G····|····x····b·········
01080¬N··Í························/usr/lib/dyld·······T·······························
01200············!·····················4··················/usr/lib/libgcc_s.1.dylib········4·············
01305·o·····/usr/lib/libSystem.B.dylib···········Pb···P·························
01425·································································
01545·································································
01665·································································
01785·································································
01905·································································
02025·································································
02145·································································
02265·································································
02385·································································
02505·································································
02625·································································
02745·································································
```

mobile\Single Files\iPhone 3-15 and 3-16 dump\AFC Service\bin\chmod (PS 0 LS 0 CL 0 SO 239 FO 0 LE 1)



Physical Analyzer

Device info:

Selected manufacturer:	Apple
Selected model:	iPhone 2G/3G/3GS
Detected manufacturer:	N/A
Detected model:	N/A
IMEI:	N/A
IMSI:	N/A

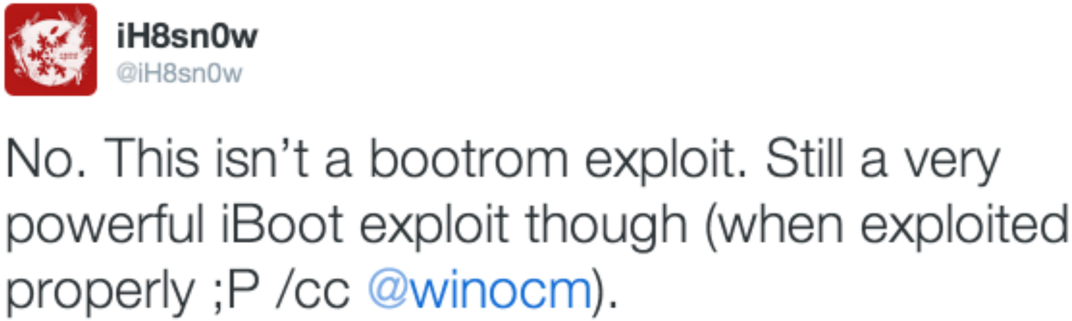
Content:

	Items	Deleted items	Total
Contacts	2447	426	2873
Call Log	101	2	103
SMS - Text Messages	48	1	49
Instant Messages (Not supported)	0	0	0
Images	25	0	25
Videos	1	0	1
Audio	397	0	397

TOOLS (IOS)

Name	Description
evasi0n / Redsn0w / ?	jailbreaking tools
TinyUmbrella	Request/playback secure signature hash (SHSH)
Cydia	AppStore for jailbroken iOS devices
OpenSSH	FOSS SSH distribution
Rbrowser	SSH/SFTP GUI for Mac ($29)
Property List Editor / plutil	Property list editor/viewer from Xcode
RazorSQL / Base	SQLite GUI clients
iPhone Analyzer	Analyze iTunes backups ~~or connect over SSH~~
PhoneView	Access data stored on your iPhone ($20)
OpenSSL	Cryptography toolkit implementing the SSL and TLS
hexedit	Hexidecimal editor/viewer
strings	Extract printable strings from binary files
Xcode	IDE for developing Mac and iOS applications

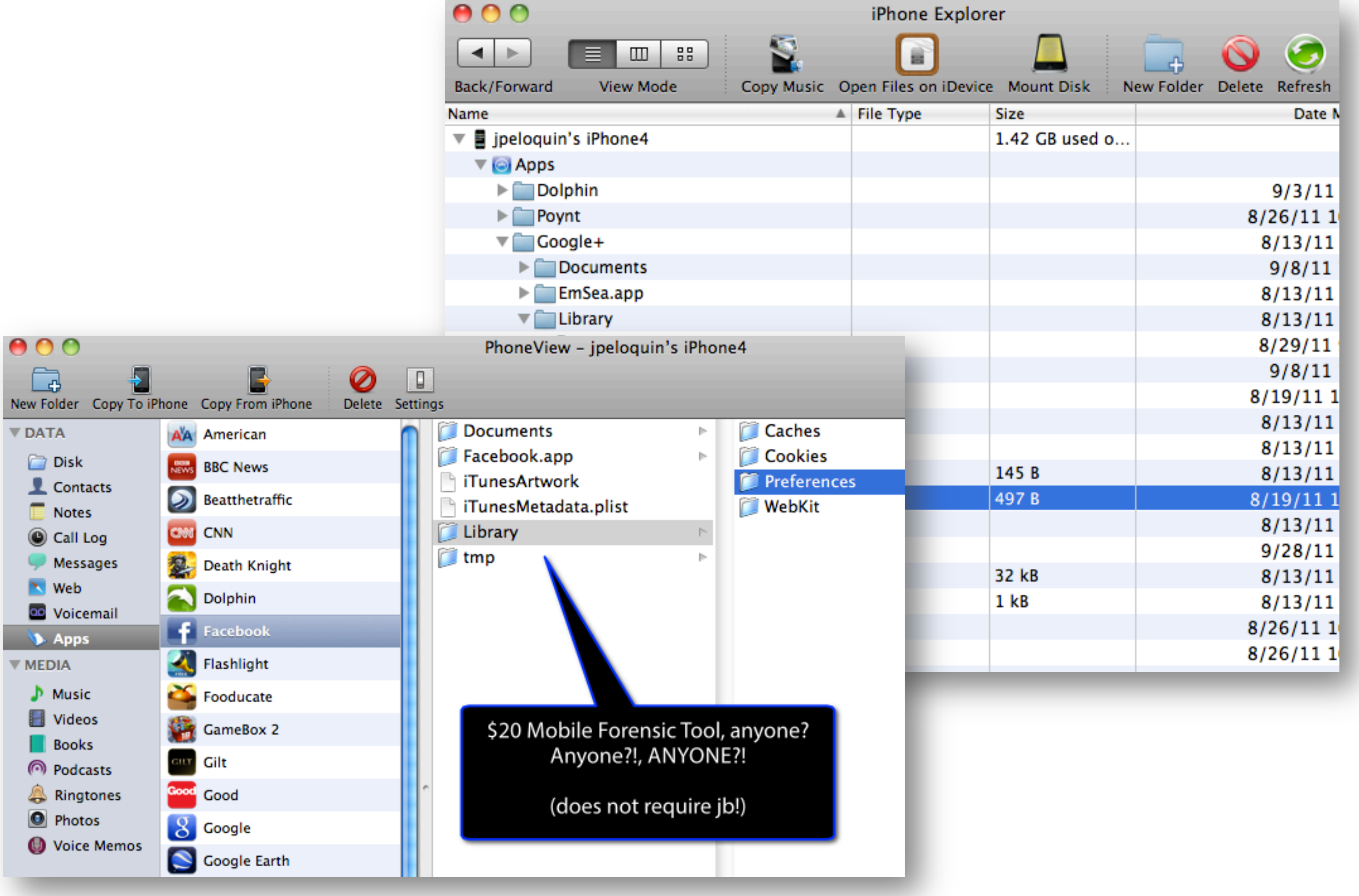
TOOLS (IOS)



iH8sn0w
@iH8sn0w

No. This isn’t a bootrom exploit. Still a very powerful iBoot exploit though (when exploited properly ;P /cc @winocm).

TOOLS (IOS)

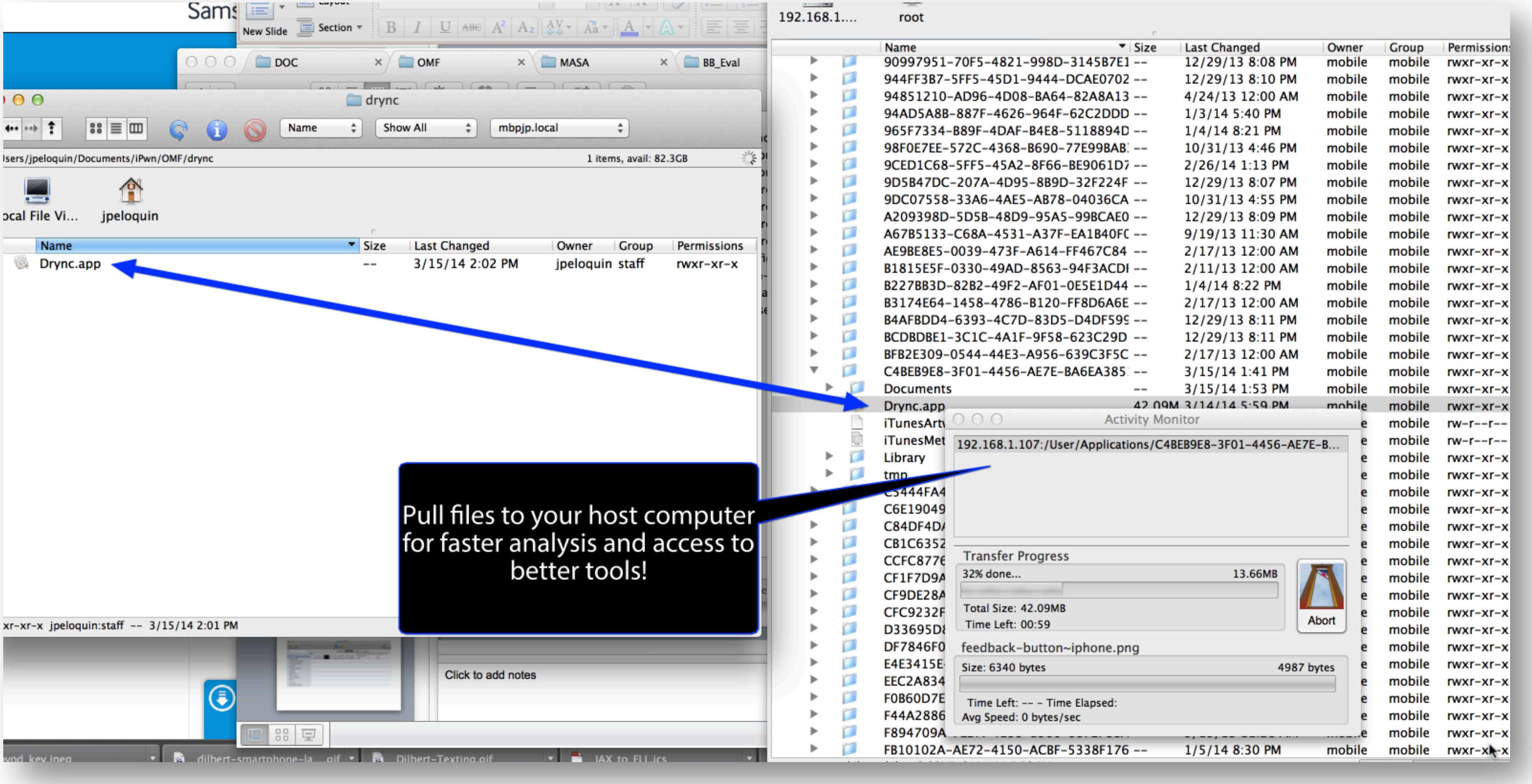


Name	File Type	Size	Date M
jpeloquin's iPhone4		1.42 GB used o…	
Apps			
Dolphin			9/3/11
Poynt			8/26/11 1
Google+			8/13/11
Documents			9/8/11
EmSea.app			8/13/11
Library			8/13/11
			8/29/11
			9/8/11
			8/19/11 1
			8/13/11
			8/13/11
		145 B	8/13/11
		497 B	8/19/11 1
			8/13/11
			9/28/11
		32 kB	8/13/11
		1 kB	8/13/11
			8/26/11 1
			8/26/11 1

$20 Mobile Forensic Tool, anyone?
Anyone?!, ANYONE?!

(does not require jb!)

TOOLS (IOS)



/Users/jpeloquin/Documents/iPwn/OMF/drync   1 items, avail: 82.3GB

Name	Size	Last Changed	Owner	Group	Permissions
Drync.app	--	3/15/14 2:02 PM	jpeloquin	staff	rwxr-xr-x

xr-xr-x jpeloquin:staff -- 3/15/14 2:01 PM

Name	Size	Last Changed	Owner	Group	Permissions
90997951-70F5-4821-998D-3145B7E1	--	12/29/13 8:08 PM	mobile	mobile	rwxr-xr-x
944FF3B7-5FF5-45D1-9444-DCAE0702	--	12/29/13 8:10 PM	mobile	mobile	rwxr-xr-x
94851210-AD96-4D08-BA64-82A8A13	--	4/24/13 12:00 AM	mobile	mobile	rwxr-xr-x
94AD5A8B-887F-4626-964F-62C2DDD	--	1/3/14 5:40 PM	mobile	mobile	rwxr-xr-x
965F7334-B89F-4DAF-B4E8-5118894D	--	1/4/14 8:21 PM	mobile	mobile	rwxr-xr-x
98F0E7EE-572C-4368-B690-77E99BAB	--	10/31/13 4:46 PM	mobile	mobile	rwxr-xr-x
9CED1C68-5FF5-45A2-8F66-BE9061D7	--	2/26/14 1:13 PM	mobile	mobile	rwxr-xr-x
9D5B47DC-207A-4D95-8B9D-32F224F	--	12/29/13 8:07 PM	mobile	mobile	rwxr-xr-x
9DC07558-33A6-4AE5-AB78-04036CA	--	10/31/13 4:55 PM	mobile	mobile	rwxr-xr-x
A209398D-5D5B-48D9-95A5-99BCAE0	--	12/29/13 8:09 PM	mobile	mobile	rwxr-xr-x
A67B5133-C68A-4531-A37F-EA1B40FC	--	9/19/13 11:30 AM	mobile	mobile	rwxr-xr-x
AE9BE8E5-0039-473F-A614-FF467C84	--	2/17/13 12:00 AM	mobile	mobile	rwxr-xr-x
B1815E5F-0330-49AD-8563-94F3ACDI	--	2/11/13 12:00 AM	mobile	mobile	rwxr-xr-x
B227BB3D-82B2-49F2-AF01-0E5E1D44	--	1/4/14 8:22 PM	mobile	mobile	rwxr-xr-x
B3174E64-1458-4786-B120-FF8D6A6E	--	2/17/13 12:00 AM	mobile	mobile	rwxr-xr-x
B4AFBDD4-6393-4C7D-83D5-D4DF59	--	12/29/13 8:11 PM	mobile	mobile	rwxr-xr-x
BCDBDBE1-3C1C-4A1F-9F58-623C29D	--	12/29/13 8:11 PM	mobile	mobile	rwxr-xr-x
BFB2E309-0544-44E3-A956-639C3F5C	--	2/17/13 12:00 AM	mobile	mobile	rwxr-xr-x
C4BEB9E8-3F01-4456-AE7E-BA6EA385	--	3/15/14 1:41 PM	mobile	mobile	rwxr-xr-x
Documents	--	3/15/14 1:53 PM	mobile	mobile	rwxr-xr-x
Drync.app	42.09M	3/14/14 5:59 PM	mobile	mobile	rwxr-xr-x
iTunesArt			e	mobile	rw-r--r--
iTunesMet			e	mobile	rw-r--r--
Library			e	mobile	rwxr-xr-x
tmp			e	mobile	rwxr-xr-x
C5444FA4			e	mobile	rwxr-xr-x
C6E19049			e	mobile	rwxr-xr-x
C84DF4D			e	mobile	rwxr-xr-x
CB1C6352			e	mobile	rwxr-xr-x
CCFC8776			e	mobile	rwxr-xr-x
CF1F7D9A			e	mobile	rwxr-xr-x
CF9DE28A			e	mobile	rwxr-xr-x
CFC9232F			e	mobile	rwxr-xr-x
D33695D			e	mobile	rwxr-xr-x
DF7846F0			e	mobile	rwxr-xr-x
E4E3415E			e	mobile	rwxr-xr-x
EEC2A834			e	mobile	rwxr-xr-x
F0B60D7E			e	mobile	rwxr-xr-x
F44A2886			e	mobile	rwxr-xr-x
F894709A			e	mobile	rwxr-xr-x
FB10102A-AE72-4150-ACBF-5338F176	--	1/5/14 8:30 PM	mobile	mobile	rwxr-xr-x

192.168.1.107:/User/Applications/C4BEB9E8-3F01-4456-AE7E-B...

Transfer Progress

32% done... 13.66MB

Total Size: 42.09MB

Time Left: 00:59

feedback-button~iphone.png

Size: 6340 bytes 4987 bytes

Time Left: -- – Time Elapsed:

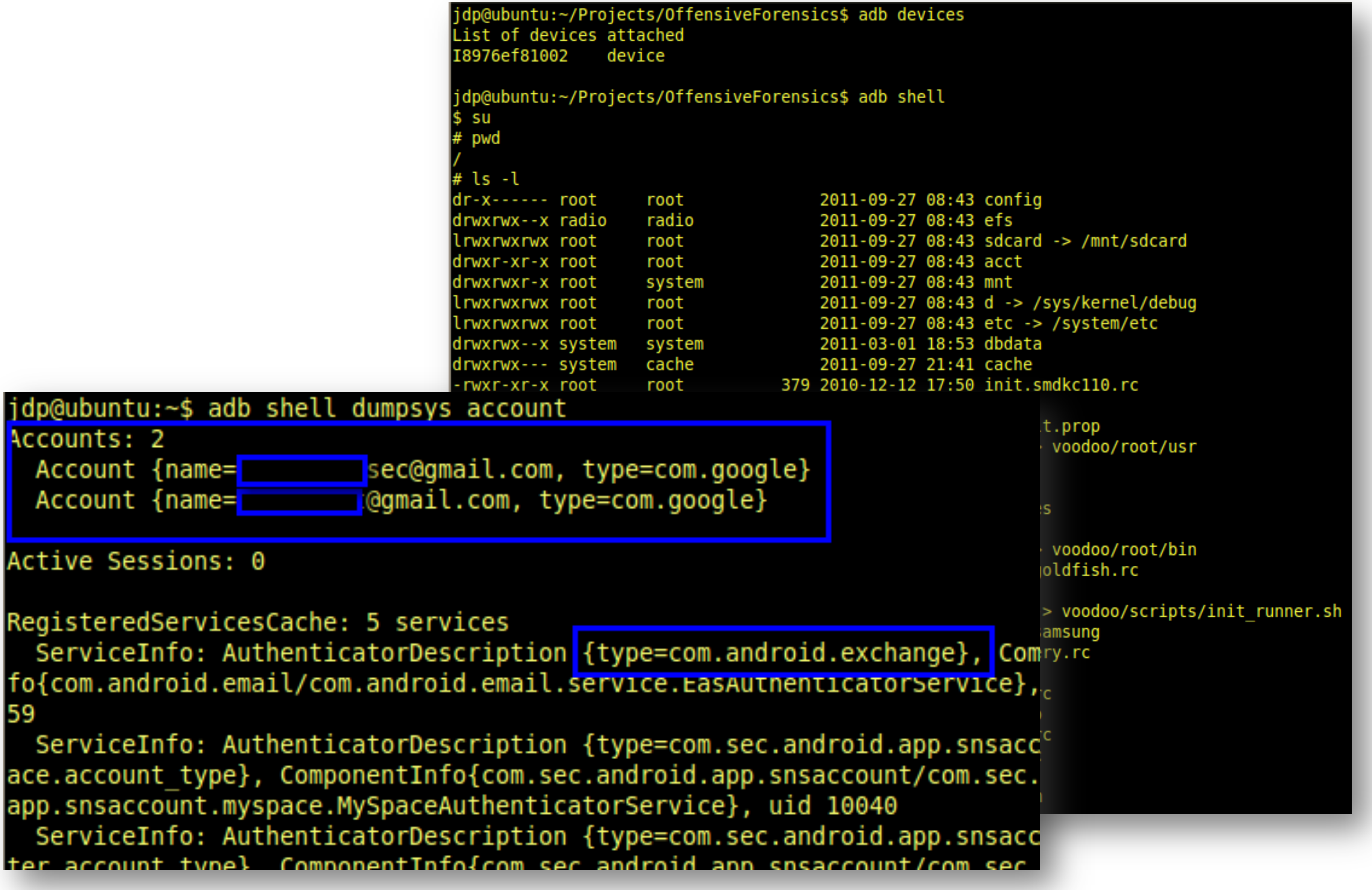
Avg Speed: 0 bytes/sec

Pull files to your host computer for faster analysis and access to better tools!

TOOLS (ANDROID)

Name	Description
Saferoot, de la Vega, NRT	Root exploits
Clockwork Recovery, TWRP	Recovery
Custom ROM	Optional
SuperSU, Busybox	Privilege escalation, linux utilities
Adbd / adb	Android debug bridge
QtADB	GUI for adb
logcat	'adb shell logcat' system and application debug msgs
dumpsys	'adb shell dumpsys' information re services, accounts
RazorSQL	SQLite GUI client
TSK	Open source digital forensics suite
hexedit	Hexidecimal editor/viewer
strings	Extract printable strings from binary files
Eclipse	IDE for developing Android applications

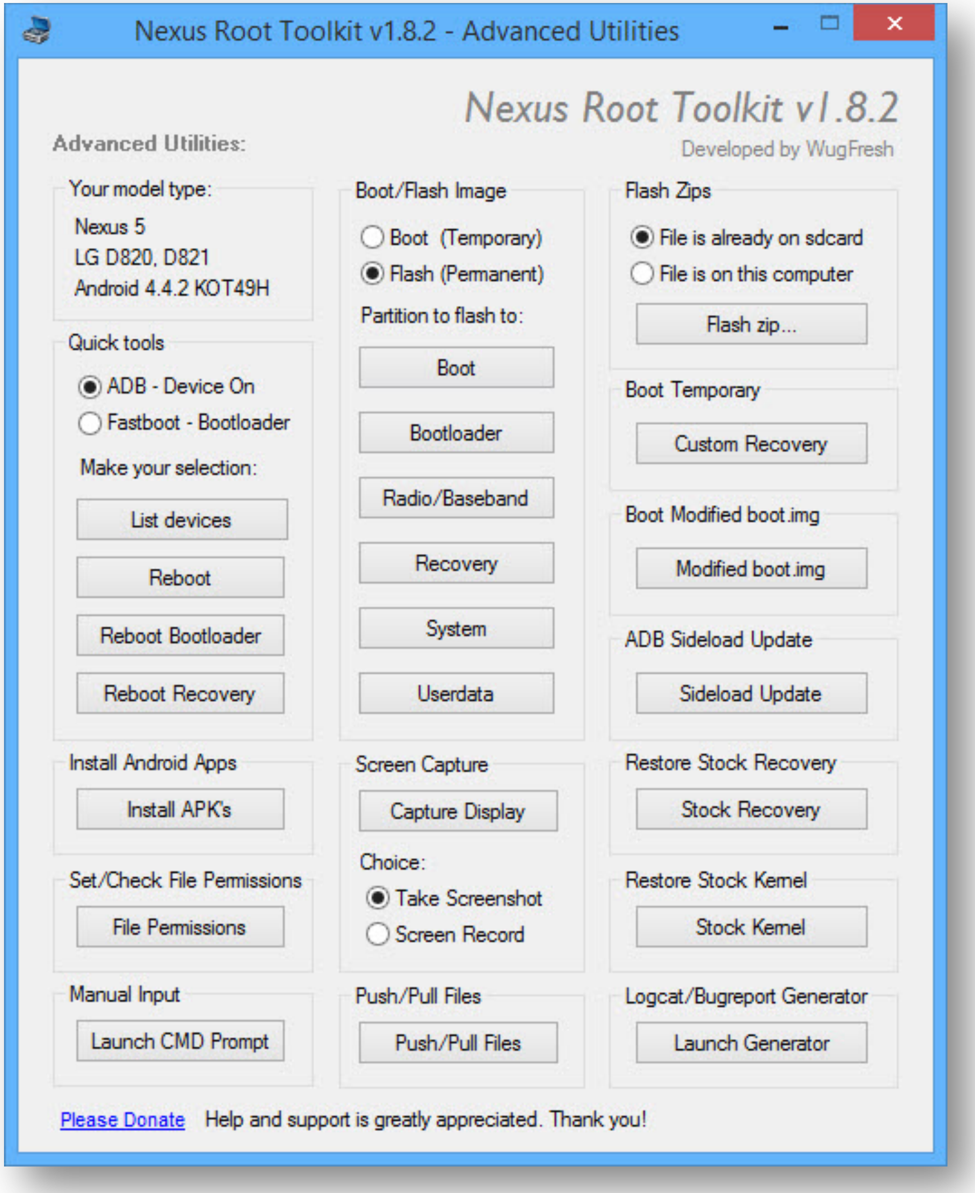
TOOLS (ANDROID)



```
jdp@ubuntu:~/Projects/OffensiveForensics$ adb devices
List of devices attached
I8976ef81002    device

jdp@ubuntu:~/Projects/OffensiveForensics$ adb shell
$ su
# pwd
/
# ls -l
dr-x------ root     root              2011-09-27 08:43 config
drwxrwx--x radio    radio             2011-09-27 08:43 efs
lrwxrwxrwx root     root              2011-09-27 08:43 sdcard -> /mnt/sdcard
drwxr-xr-x root     root              2011-09-27 08:43 acct
drwxrwxr-x root     system            2011-09-27 08:43 mnt
lrwxrwxrwx root     root              2011-09-27 08:43 d -> /sys/kernel/debug
lrwxrwxrwx root     root              2011-09-27 08:43 etc -> /system/etc
drwxrwx--x system   system            2011-03-01 18:53 dbdata
drwxrwx--- system   cache             2011-09-27 21:41 cache
-rwxr-xr-x root     root          379 2010-12-12 17:50 init.smdkc110.rc
                                                       t.prop
                                                       voodoo/root/usr

                                                       s

                                                       voodoo/root/bin
                                                       oldfish.rc

                                                       > voodoo/scripts/init_runner.sh
                                                       amsung
                                                       ry.rc
                                                       c

                                                       c
```

```
jdp@ubuntu:~$ adb shell dumpsys account
Accounts: 2
  Account {name=[redacted]sec@gmail.com, type=com.google}
  Account {name=[redacted]@gmail.com, type=com.google}

Active Sessions: 0

RegisteredServicesCache: 5 services
  ServiceInfo: AuthenticatorDescription {type=com.android.exchange}, Com
fo{com.android.email/com.android.email.service.EasAuthenticatorService},
59
  ServiceInfo: AuthenticatorDescription {type=com.sec.android.app.snsacc
ace.account_type}, ComponentInfo{com.sec.android.app.snsaccount/com.sec.
app.snsaccount.myspace.MySpaceAuthenticatorService}, uid 10040
  ServiceInfo: AuthenticatorDescription {type=com.sec.android.app.snsacc
ter_account_type}, ComponentInfo{com.sec.android.app.snsaccount/com.sec
```

TOOLS (ANDROID)



Nexus Root Toolkit v1.8.2 - Advanced Utilities

Nexus Root Toolkit v1.8.2

Developed by WugFresh

Advanced Utilities:

Your model type:

Nexus 5
LG D820, D821
Android 4.4.2 KOT49H

Quick tools

● ADB - Device On
○ Fastboot - Bootloader

Make your selection:

Boot/Flash Image

○ Boot (Temporary)
● Flash (Permanent)

Partition to flash to:

Flash Zips

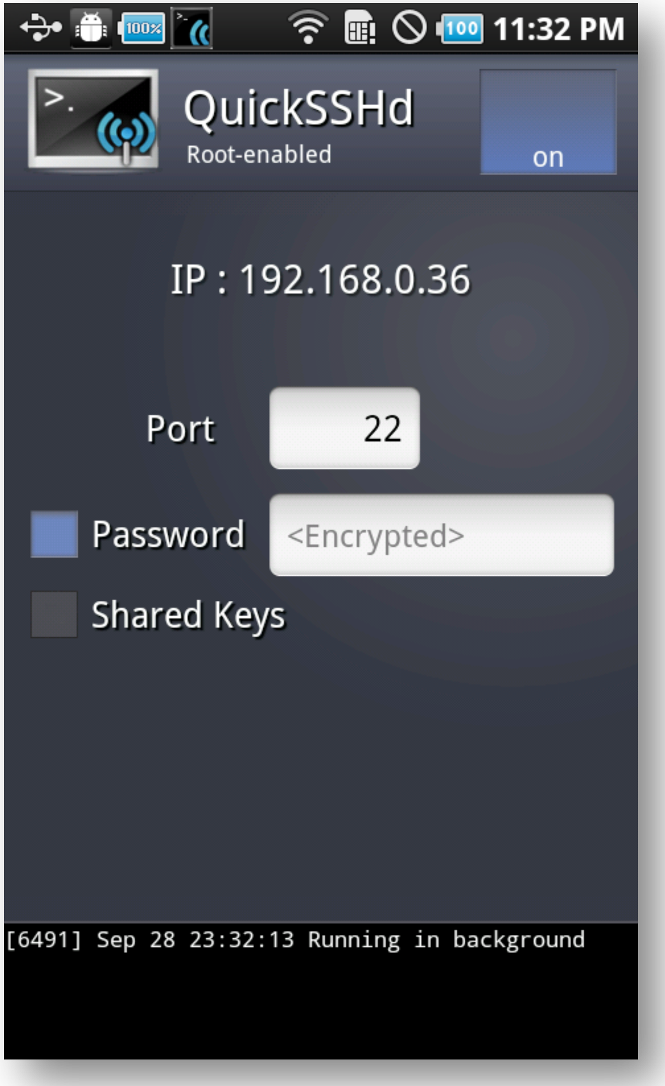
● File is already on sdcard
○ File is on this computer

Screen Capture

Choice:

● Take Screenshot
○ Screen Record

Please Donate Help and support is greatly appreciated. Thank you!



11:32 PM

QuickSSHd

Root-enabled

on

IP : 192.168.0.36

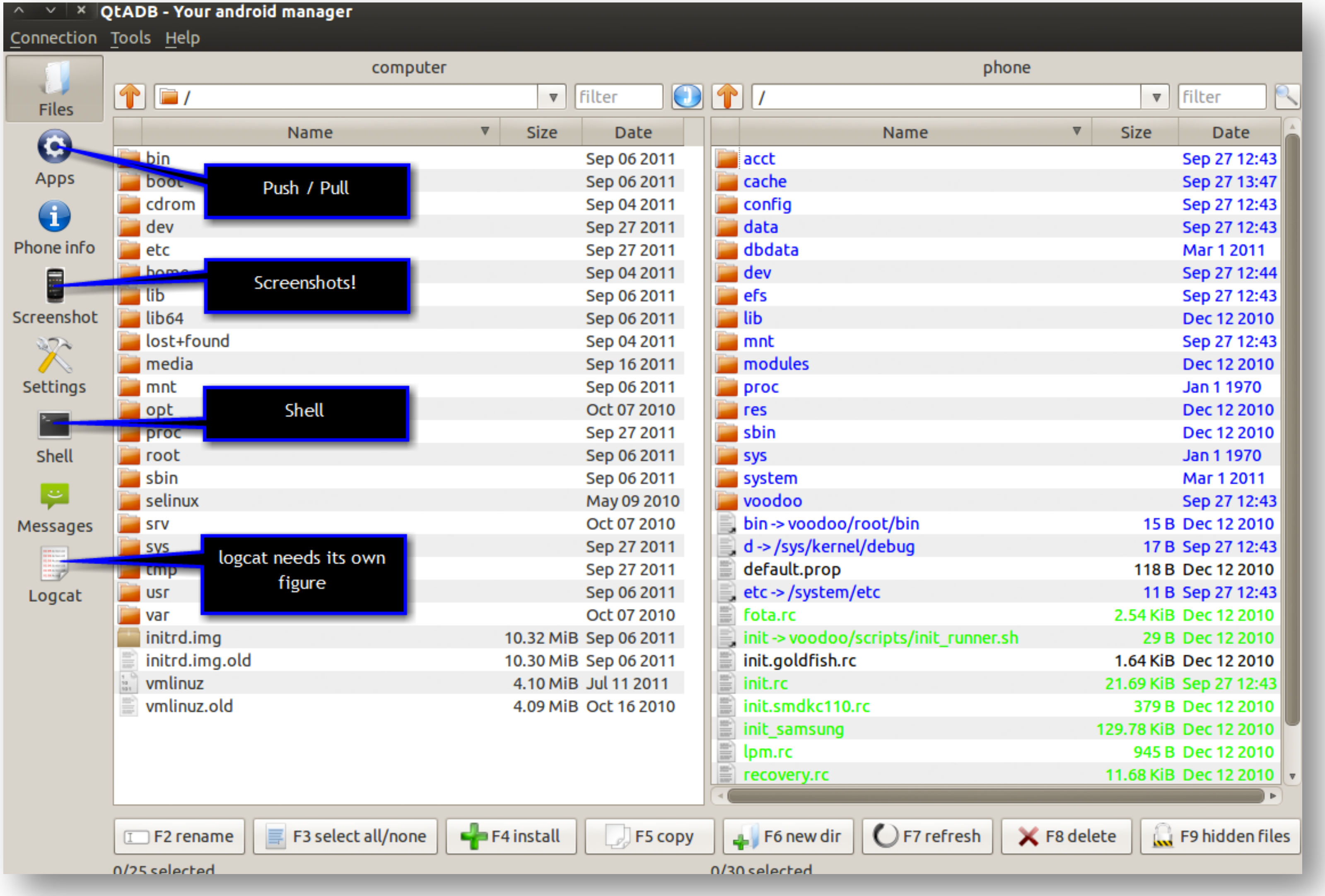
Port 22

☑ Password <Encrypted>

□ Shared Keys

```
[6491] Sep 28 23:32:13 Running in background
```

TOOLS (ANDROID)



Push / Pull

Screenshots!

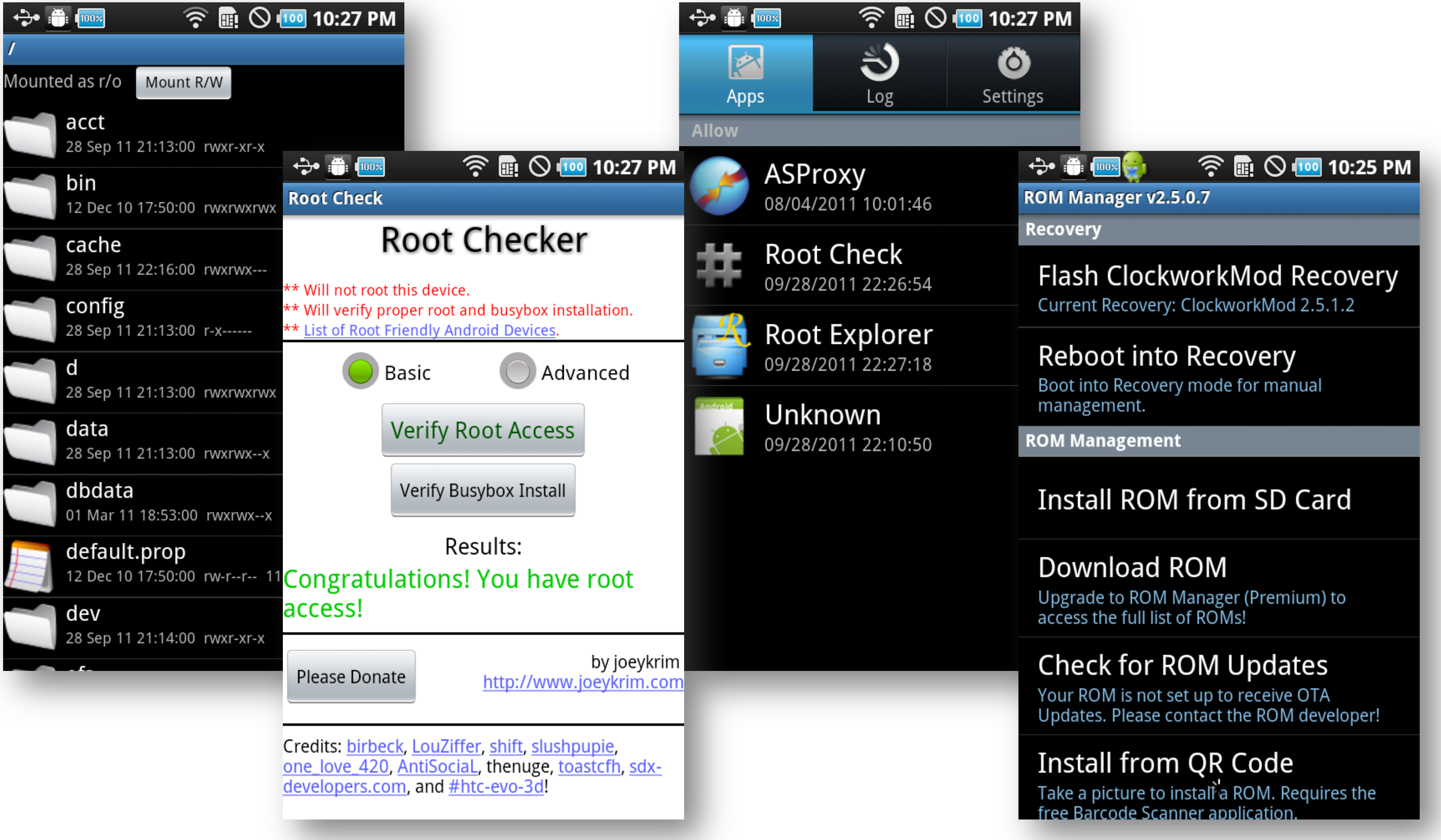
Shell

logcat needs its own figure

Name	Size	Date
bin		Sep 06 2011
boot		Sep 06 2011
cdrom		Sep 04 2011
dev		Sep 27 2011
etc		Sep 27 2011
home		Sep 04 2011
lib		Sep 06 2011
lib64		Sep 06 2011
lost+found		Sep 04 2011
media		Sep 16 2011
mnt		Sep 06 2011
opt		Oct 07 2010
proc		Sep 27 2011
root		Sep 06 2011
sbin		Sep 06 2011
selinux		May 09 2010
srv		Oct 07 2010
sys		Sep 27 2011
tmp		Sep 27 2011
usr		Sep 06 2011
var		Oct 07 2010
initrd.img	10.32 MiB	Sep 06 2011
initrd.img.old	10.30 MiB	Sep 06 2011
vmlinuz	4.10 MiB	Jul 11 2011
vmlinuz.old	4.09 MiB	Oct 16 2010

Name	Size	Date
acct		Sep 27 12:43
cache		Sep 27 13:47
config		Sep 27 12:43
data		Sep 27 12:43
dbdata		Mar 1 2011
dev		Sep 27 12:44
efs		Sep 27 12:43
lib		Dec 12 2010
mnt		Sep 27 12:43
modules		Dec 12 2010
proc		Jan 1 1970
res		Dec 12 2010
sbin		Dec 12 2010
sys		Jan 1 1970
system		Mar 1 2011
voodoo		Sep 27 12:43
bin -> voodoo/root/bin	15 B	Dec 12 2010
d -> /sys/kernel/debug	17 B	Sep 27 12:43
default.prop	118 B	Dec 12 2010
etc -> /system/etc	11 B	Sep 27 12:43
fota.rc	2.54 KiB	Dec 12 2010
init -> voodoo/scripts/init_runner.sh	29 B	Dec 12 2010
init.goldfish.rc	1.64 KiB	Dec 12 2010
init.rc	21.69 KiB	Sep 27 12:43
init.smdkc110.rc	379 B	Dec 12 2010
init_samsung	129.78 KiB	Dec 12 2010
lpm.rc	945 B	Dec 12 2010
recovery.rc	11.68 KiB	Dec 12 2010

TOOLS (ANDROID)



10:27 PM

/

Mounted as r/o

```
acct
28 Sep 11 21:13:00  rwxr-xr-x
bin
12 Dec 10 17:50:00  rwxrwxrwx
cache
28 Sep 11 22:16:00  rwxrwx---
config
28 Sep 11 21:13:00  r-x------
d
28 Sep 11 21:13:00  rwxrwxrwx
data
28 Sep 11 21:13:00  rwxrwx--x
dbdata
01 Mar 11 18:53:00  rwxrwx--x
default.prop
12 Dec 10 17:50:00  rw-r--r--  11
dev
28 Sep 11 21:14:00  rwxr-xr-x
```

10:27 PM

Root Check

Root Checker

** Will not root this device.
** Will verify proper root and busybox installation.
** List of Root Friendly Android Devices.

● Basic ○ Advanced

Results:

Congratulations! You have root access!

by joeykrim
http://www.joeykrim.com

Credits: birbeck, LouZiffer, shift, slushpupie, one_love_420, AntiSociaL, thenuge, toastcfh, sdx-developers.com, and #htc-evo-3d!

10:27 PM

Allow

ASProxy	08/04/2011 10:01:46
Root Check	09/28/2011 22:26:54
Root Explorer	09/28/2011 22:27:18
Unknown	09/28/2011 22:10:50

10:25 PM

ROM Manager v2.5.0.7

Recovery

Flash ClockworkMod Recovery
Current Recovery: ClockworkMod 2.5.1.2

Reboot into Recovery
Boot into Recovery mode for manual management.

ROM Management

Install ROM from SD Card

Download ROM
Upgrade to ROM Manager (Premium) to access the full list of ROMs!

Check for ROM Updates
Your ROM is not set up to receive OTA Updates. Please contact the ROM developer!

Install from QR Code
Take a picture to install a ROM. Requires the free Barcode Scanner application.

GOT DATA?

(IOS)

LOC DATA (IOS)

4.3.2

Location	Description
/var/mobile/Library/AddressBook/AddressBook.sqlitedb	also AddressBookImages.sqlitedb
/var/mobile/Library/Caches/MapTiles/MapTiles.sqlitedb	previously displayed map tiles for Google Maps "binhex" encoding - covert to binary
/var/mobile/Library/Maps/History.plist	google maps lookup cache - check Directions.plist as well
/var/mobile/Library/Calendar/Calendar.sqlitedb	sqlclient / strings
/var/mobile/Library/Callhistory/call_history.db	sqlclient / strings / odd number (FLAGS) outgoing, even incoming
/var/mobile/Library/Mail/Envelope Index	
/var/mobile/Library/Notes/notes.sqlite	sqlclient / strings
/var/mobile/Library/SMS/sms.db	sqlclient / strings / FLAGS-low order bit set for sent (odd), off for received (even)
/var/mobile/Library/Voicemail/voicemail.db	voicemail database
/var/mobile/Library/Voicemail/	vm recordings
/var/mobile/Library/Cookies/Cookies.binarycookies	Safari cookies - use strings
/var/mobile/Library/Preferences	settings, config files for apps
/var/mobile/Library/Safari/Bookmarks.db	
/var/mobile/Library/Safari/History.plist	
/var/mobile/Library/Safari/SuspendState.plist	browser state when closed, crashed, etc.
/var/mobile/Library/Preferences/com.apple.mobilesafari.plist	
/var/mobile/Media/DCIM/100APPLE	photos taken with onboard camera
/var/mobile/Library/Logs	
/var/mobileDevice/ProvisioningProfiles	
/var/log	
/var/logs	
/var/preferences/SystemConfiguration/com.apple.network.identification.plist	
/var/preferences/SystemConfiguration/com.apple.wifi.plist	
/var/preferences/SystemConfiguration/preferences.plist	
/var/stash	ringtones, wallpaper, default apps, /bin dir
/var/wireless/Library/CallHistory	
/var/wireless/Library/logs	
/var/wireless/Library/Preferences	
/root/Library/Lockdown/data_ark.plist	apple id, owner info, firmware
/var/Keychains	download keychains databases

LOC DATA (IOS)

4.3.2

Location	Description
/User/Library/Keyboard/dynamic-text.dat	analyze keyboard cache
/User/Library/Caches/com.apple.UIKit.pboard/pasteboardDB	convert to XML to analyze pasteboard cache
/User/Library/Caches/com.apple.WebAppCache/ApplicationCache.db	Origins table
/User/Library/Caches/Snapshots	Pics of apps when Home is pressed
/User/Applications	user-installed applications
/User/Applications/<app GUID>/<appname.app>	app assets - nibs, images, plists, code signature, etc.
/User/Applications/<app GUID>/Documents	images, text files, etc
/User/Applications/<app GUID>/Library	
/User/Applications/<app GUID>/Library/Caches	
/User/Applications/<app GUID>/Library/Caches/Snapshots	
/User/Applications/<app GUID>/Library/Cookies/Cookies.binarycookies	
/User/Applications/<app GUID>/Library/Preferences	plists-a-plenty
/User/Applications/<app GUID>/Library/WebKit	
/User/Applications/<app GUID>/Library/WebKit/LocalStorage	
/User/Applications/<app GUID>/tmp	
/User/Library/Logs/CrashReporter	Application crash logs

LOC DATA (IOS)

5.1.1

Location	Description
/var/mobile/Library/AddressBook/AddressBook.sqlitedb	also AddressBookImages.sqlitedb
/var/mobile/Library/Caches/MapTiles/MapTiles.sqlitedb	previously displayed map tiles for Google Maps "binhex" encoding - covert to binary
/var/mobile/Library/Maps/History.plist	google maps lookup cache - check Directions.plist as well
/var/mobile/Library/Calendar/Calendar.sqlitedb	sqlclient / strings
/var/mobile/Library/Callhistory/call_history.db	sqlclient / strings / odd number (FLAGS) outgoing, even incoming
/var/mobile/Library/Mail/Envelope Index	
/var/mobile/Library/Notes/notes.sqlite	sqlclient / strings
/var/mobile/Library/SMS/sms.db	sqlclient / strings / FLAGS-low order bit set for sent (odd), off for received (even)
/var/mobile/Library/Voicemail/voicemail.db	voicemail database
/var/mobile/Library/Voicemail/	vm recordings
/var/mobile/Library/Cookies/Cookies.binarycookies	Safari cookies - use strings
/var/mobile/Library/Preferences	settings, config files for apps
/var/mobile/Library/Safari/Bookmarks.db	
/var/mobile/Library/Safari/History.plist	
/var/mobile/Library/Safari/SuspendState.plist	browser state when closed, crashed, etc.
/var/mobile/Library/Preferences/com.apple.mobilesafari.plist	
/var/mobile/Media/DCIM/100APPLE	photos taken with onboard camera
/var/mobile/Library/Logs	
/var/mobileDevice/ProvisioningProfiles	
/var/log	
/var/logs	
/var/preferences/SystemConfiguration/com.apple.network.identification.plist	
/var/preferences/SystemConfiguration/com.apple.wifi.plist	
/var/preferences/SystemConfiguration/preferences.plist	
/var/stash	ringtones, wallpaper, default apps, /bin dir
/var/wireless/Library/CallHistory	
/var/wireless/Library/logs	
/var/wireless/Library/Preferences	
/root/Library/Lockdown/data_ark.plist	apple id, owner info, firmware
/var/Keychains	download keychains databases

LOC DATA (IOS)

5.1.1

Location	Description
/var/Keychains	download keychains databases
/var/mobile/Library/Caches/com.apple.dataaccess.dataaccessd	iCloud login ID and persistent server
/var/mobile/Library/Caches/com.apple.mobilecal	?
/var/mobile/Library/Caches/com.apple.mobilemail	mobile mail image blobs + URLs
/var/mobile/Library/Caches/com.apple.mobilenotes	?
/var/mobile/Library/Caches/com.apple.mobilesafari	Cached images + URLs from Safari
/var/mobile/Library/Caches/Maps/MapTiles	db of previously displayed maptiles (google maps)
/var/mobile/Library/Caches/Safari/RecentSearches.plist	Recent search strings from Safari. Also check the Thumbnails subfolder for snapshots.
/var/mobile/Library/Caches/Snapshots	Last screens for camera, mmail, mcal, mnotes, mphone, and many others.
/User/Library/Caches/com.apple.WebAppCache/ApplicationCache.db	Origins table
/User/Applications	user-installed applications
/User/Applications/<app GUID>/<appname.app>	app assets - nibs, images, plists, code signature, etc.
/User/Applications/<app GUID>/Documents	images, text files, etc
/User/Applications/<app GUID>/Library	
/User/Applications/<app GUID>/Library/Caches	
/User/Applications/<app GUID>/Library/Caches/Snapshots	pic of the app's state when home button pushed
/User/Applications/<app GUID>/Library/Cookies/Cookies.binarycookies	
/User/Applications/<app GUID>/Library/Preferences	plists-a-plenty
/User/Applications/<app GUID>/Library/WebKit	
/User/Applications/<app GUID>/Library/WebKit/LocalStorage	
/User/Applications/<app GUID>/tmp	

LOC DATA (IOS)

6.1.2

Location	Description
/var/mobile/Library/AddressBook/AddressBook.sqlitedb	also AddressBookImages.sqlitedb
/var/mobile/Library/Caches/MapTiles/MapTiles.sqlitedb	previously displayed map tiles for Google Maps "binhex" encoding - covert to binary
/var/mobile/Library/Maps/	google maps lookup cache, Directions, bookmarks
/var/mobile/Library/Calendar/Calendar.sqlitedb	sqlclient / strings
/var/mobile/Library/DataAccess	IMAP accounts
/var/mobile/Library/Mail/	personal and corporate mail, icloud
/var/mobile/Library/Notes/notes.sqlite	pull written notes out of db - sqlclient / strings
/var/mobile/Library/SMS/sms.db	sqlclient / strings / FLAGS-low order bit set for sent (odd), off for received (even)
/var/mobile/Library/Keyboard	dynamic-text.dat - use strings, CloudUserDictionary.sqlite
/var/mobile/Library/Voicemail/	vm recordings and voicemail database (metadata)
/var/mobile/Library/Cookies/Cookies.binarycookies	Safari cookies - use strings
/var/mobile/Library/Preferences	settings, config files for apps
/var/mobile/Library/Safari/	bookmarks, history, browser state when closed or crashed, etc.
/var/mobile/Library/Mobile Documents	keynote and pdf reader - neither using the folders
/var/mobile/Library/Preferences/com.apple.mobilesafari.plist	
/var/mobile/Media/DCIM/100APPLE	photos taken with onboard camera
/var/mobile/Library/Logs	support, itunes, facetime, siri, etc.
/var/mobileDevice/ProvisioningProfiles	Provisioned enterprise apps
/var/log	kernel, ppp, jb
/var/logs	keybag, lockdown
/var/preferences/SystemConfiguration/ com.apple.network.identification.plist	ALL networks this device has ever connected to
/var/preferences/SystemConfiguration/com.apple.wifi.plist	ALL wifi networks (SSID, etc.) this device has ever connected to
/var/preferences/SystemConfiguration/preferences.plist	Interesting network information. VPN clients that save passwd and fail to encrypt outed here.
/var/stash	ringtones, wallpaper, default apps, /bin dir
/var/wireless/Library/CallHistory	call_history.db
/var/wireless/Library/Logs	core, baseband
/var/wireless/Library/Preferences	commCenter
/root/Library/Lockdown/data_ark.plist	apple id, owner info, firmware
/var/keybags	Master keys for protection classes (AES)

LOC DATA (IOS)

6.1.2

Location	Description
/var/Keychains	download keychains databases
/var/mobile/Library/Caches/com.apple.dataaccess.dataaccessd	iCloud login ID and persistent server
/var/mobile/Library/Caches/com.apple.mobilecal	?
/var/mobile/Library/Caches/com.apple.mobilemail	mobile mail image blobs + URLs
/var/mobile/Library/Caches/com.apple.mobilenotes	?
/var/mobile/Library/Caches/com.apple.mobilesafari	Cached images + URLs from Safari
/var/mobile/Library/Caches/Maps/MapTiles	db of previously displayed maptiles (google maps)
/var/mobile/Library/Caches/Safari/RecentSearches.plist	Displays recent search strings from Safari. Also check the Thumbnails subfolder for snapshots.
/var/mobile/Library/Caches/Snapshots	Last screens for camera, mmail, mcal, mnotes, mphone, and many others.
/User/Library/Caches/com.apple.WebAppCache/ApplicationCache.db	Origins table
/User/Applications	user-installed applications
/User/Applications/<app GUID>/<appname.app>	app assets - nibs, images, plists, code signature, etc.
/User/Applications/<app GUID>/Documents	images, text files, etc
/User/Applications/<app GUID>/Library	
/User/Applications/<app GUID>/Library/Caches	
/User/Applications/<app GUID>/Library/Caches/Snapshots	pic of the app's state when home button pushed
/User/Applications/<app GUID>/Library/Cookies/Cookies.binarycookies	
/User/Applications/<app GUID>/Library/Preferences	plists-a-plenty
/User/Applications/<app GUID>/Library/WebKit	
/User/Applications/<app GUID>/Library/WebKit/LocalStorage	
/User/Applications/<app GUID>/tmp	
/var/mobile/Library/Accounts/Accounts3.sqlite	**gmail, icloud, twitter,etc., accounts**
/var/mobile/Library/Application Support/Ubiquity/peer-*	**item-info.db**
/var/mobile/Library/Assistant/ManagedObjects.sqlite	**Siri-used reminders - use strings, e.g. "Call lawn care service America/New_York"**
/var/mobile/Library/DataAccess	**IMAP, iCloud accounts**
/var/mobile/Library/Passes	**Passbook - Flight, Hotel info**

LOC DATA (IOS)

7.0.6

Location	Description
/var/mobile/Library/AddressBook/AddressBook.sqlitedb	also AddressBookImages.sqlitedb
/var/mobile/Library/Caches/MapTiles/MapTiles.sqlitedb	previously displayed map tiles for Google Maps "binhex" encoding - covert to binary
/var/mobile/Library/Maps/	google maps lookup cache, Directions, bookmarks
/var/mobile/Library/Calendar/Calendar.sqlitedb	sqlclient / strings
/var/mobile/Library/DataAccess	IMAP accounts
/var/mobile/Library/Mail/	personal and corporate mail, icloud
/var/mobile/Library/Notes/notes.sqlite	pull written notes out of db - sqlclient / strings
/var/mobile/Library/SMS/sms.db	sqlclient / strings / FLAGS-low order bit set for sent (odd), off for received (even)
/var/mobile/Library/Keyboard	dynamic-text.dat - use strings, CloudUserDictionary.sqlite
/var/mobile/Library/Voicemail/	vm recordings and voicemail database (metadata)
/var/mobile/Library/Cookies/Cookies.binarycookies	Safari cookies - use strings
/var/mobile/Library/Preferences	settings, config files for apps
/var/mobile/Library/Safari/	bookmarks, history, browser state when closed or crashed, etc.
/var/mobile/Library/Mobile Documents	keynote and pdf reader - neither using the folders
/var/mobile/Media/DCIM/100APPLE	photos taken with onboard camera
/var/mobile/Library/Logs	support, itunes, facetime, siri, etc.
/Library/MobileDevice/ProvisioningProfiles	Provisioned enterprise apps
/var/mobile/Library/Caches/com.apple.UIKit.pboard	Copy/paste buffer
/Library/Logs	kernel, ppp, jb, keybag, lockdown
/Library/Preferences/SystemConfiguration/com.apple.network.identification.plist	ALL networks this device has ever connected to
/Library/Preferences/SystemConfiguration/com.apple.wifi.plist	ALL wifi networks (SSID, etc.) this device has ever connected to
/Library/Preferences/SystemConfiguration/preferences.plist	Interesting network information. VPN clients that save passwd and fail to encrypt outed here.
/var/stash	ringtones, wallpaper, default apps
/var/wireless/Library/CallHistory	call_history.db
/var/wireless/Library/Logs	core, baseband
/root/Library/Lockdown/data_ark.plist	apple id, owner info, firmware
/var/keybags	Master keys for protection classes (AES)

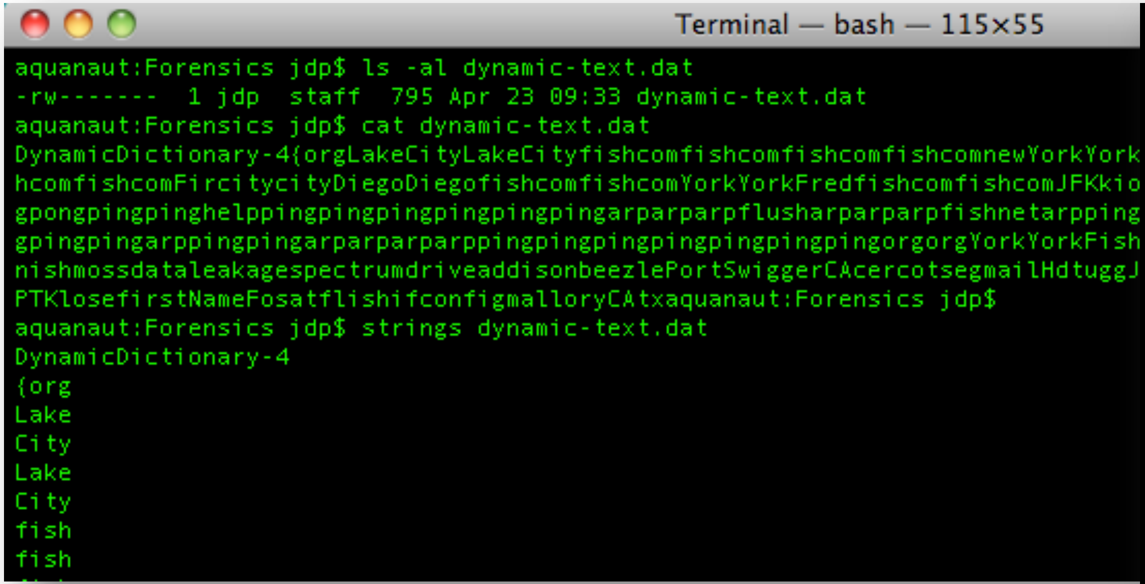
LOC DATA (IOS)

7.0.6

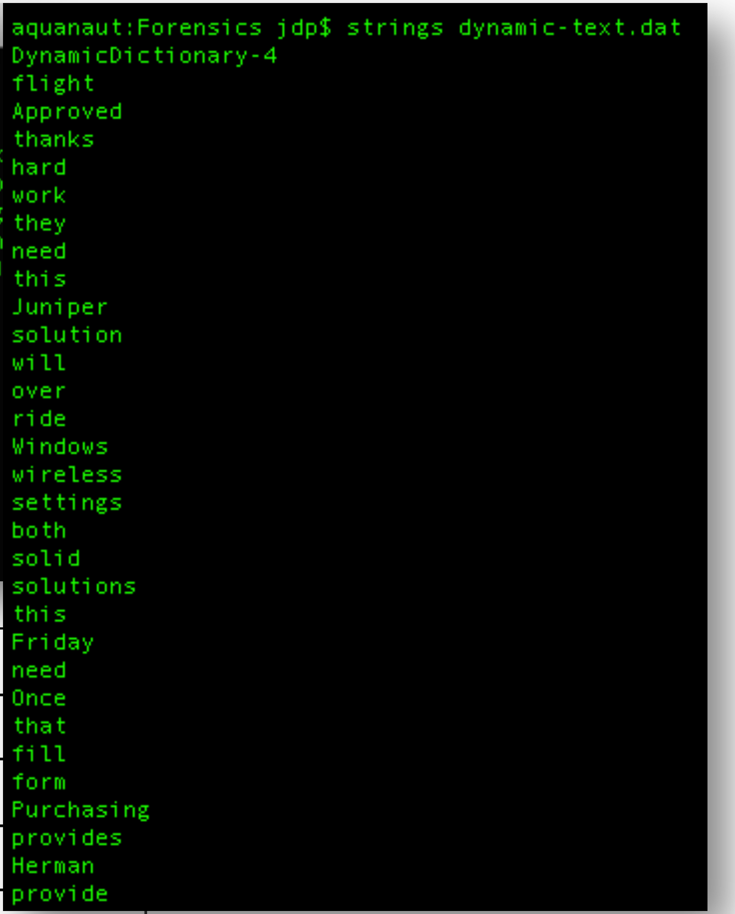
Location	Description
/var/Keychains	download keychains databases
/var/mobile/Library/Caches/com.apple.dataaccess.dataaccessd	iCloud login ID and persistent server
/var/mobile/Library/Caches/com.apple.mobilecal	
/var/mobile/Library/Caches/com.apple.mobilemail	Complete emaill threads; sender/recipient, message, attachments
/var/mobile/Library/Caches/com.apple.mobilenotes	
/var/mobile/Library/Caches/com.apple.mobilesafari	Thumbnails,ad URI cache, recent searches (plist)
/var/mobile/Library/Caches/Maps/MapTiles	db of previously displayed maptiles (google maps)
/var/mobile/Library/Caches/Safari/RecentSearches.plist	Displays recent search strings from Safari. Also check the Thumbnails subfolder for snapshots.
/var/mobile/Library/Caches/Snapshots	Last screens for camera, mmail, mcal, mnotes, mphone, and many others.
/User/Library/Caches/com.apple.WebAppCache/ApplicationCache.db	Origins table
/User/Applications	user-installed applications
/User/Applications/<app GUID>/<appname.app>	app assets - nibs, images, plists, code signature, etc.
/User/Applications/<app GUID>/Documents	images, text files, etc
/User/Applications/<app GUID>/Library	
/User/Applications/<app GUID>/Library/Caches	
/User/Applications/<app GUID>/Library/Caches/Snapshots	pic of the app's state when home button pushed
/User/Applications/<app GUID>/Library/Cookies/Cookies.binarycookies	
/User/Applications/<app GUID>/Library/Preferences	plists-a-plenty
/User/Applications/<app GUID>/Library/WebKit	
/User/Applications/<app GUID>/Library/WebKit/LocalStorage	
/User/Applications/<app GUID>/tmp	
/var/mobile/Library/Accounts/Accounts3.sqlite	gmail, icloud, twitter,etc., accounts
/var/mobile/Library/Application Support/Ubiquity/peer-*	item-info.db
/var/mobile/Library/Assistant/ManagedObjects.sqlite	Siri-used reminders - use strings, e.g. "Call lawn care service America/New_York"
/var/mobile/Library/DataAccess	IMAP, iCloud accounts
/var/mobile/Library/Passes	Passbook - Flight, Hotel info

IOS FINDINGS!

KEYBOARD CACHE



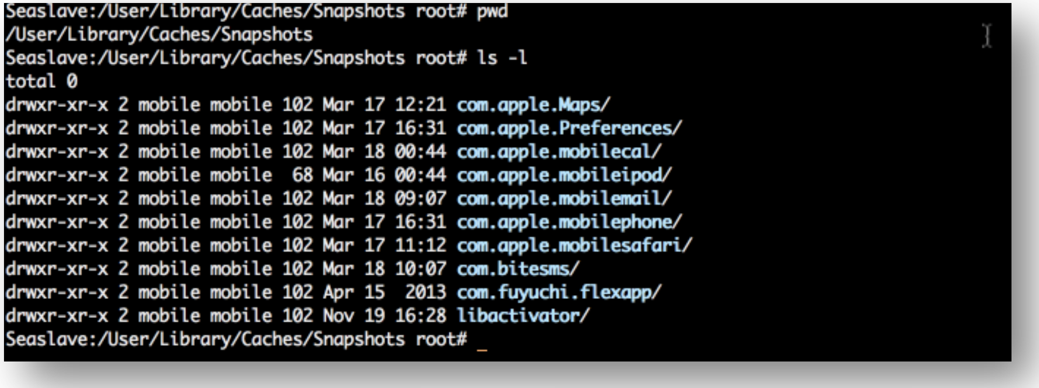
```
aquanaut:Forensics jdp$ ls -al dynamic-text.dat
-rw-------  1 jdp  staff  795 Apr 23 09:33 dynamic-text.dat
aquanaut:Forensics jdp$ cat dynamic-text.dat
DynamicDictionary-4{orgLakeCityLakeCityfishcomfishcomfishcomfishcomnewYorkYork
hcomfishcomFircitycityDiegoDiegofishcomfishcomYorkYorkFredfishcomfishcomJFKkio
gpongpingpinghelppingpingpingpingpingpingarparparpflusharparparpfishnetarpping
gpingpingarppingpingarparparparppingpingpingpingpingpingpingorgorgYorkYorkFish
nishmossdataleakagespectrumdriveaddisonbeezlePortSwiggerCAercotsegmailHdtuggJ
PTKlosefirstNameFosatflishifconfigmalloryCAtxaquanaut:Forensics jdp$
aquanaut:Forensics jdp$ strings dynamic-text.dat
DynamicDictionary-4
{org
Lake
City
Lake
City
fish
fish
```



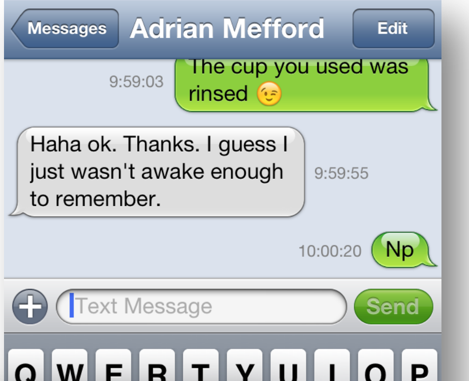
```
aquanaut:Forensics jdp$ strings dynamic-text.dat
DynamicDictionary-4
flight
Approved
thanks
hard
work
they
need
this
Juniper
solution
will
over
ride
Windows
wireless
settings
both
solid
solutions
this
Friday
need
Once
that
fill
form
Purchasing
provides
Herman
provide
```

amit	just	work	also
will	need	with	could
have	make	larry	have
coordinate	sure	governance	copied
that	that	risk	yourself
through	case	compliance	
help	available		
desk			

SNAPSHOTS



```
Seaslave:/User/Library/Caches/Snapshots root# pwd
/User/Library/Caches/Snapshots
Seaslave:/User/Library/Caches/Snapshots root# ls -l
total 0
drwxr-xr-x 2 mobile mobile 102 Mar 17 12:21 com.apple.Maps/
drwxr-xr-x 2 mobile mobile 102 Mar 17 16:31 com.apple.Preferences/
drwxr-xr-x 2 mobile mobile 102 Mar 18 00:44 com.apple.mobilecal/
drwxr-xr-x 2 mobile mobile  68 Mar 16 00:44 com.apple.mobileipod/
drwxr-xr-x 2 mobile mobile 102 Mar 18 09:07 com.apple.mobilemail/
drwxr-xr-x 2 mobile mobile 102 Mar 17 16:31 com.apple.mobilephone/
drwxr-xr-x 2 mobile mobile 102 Mar 17 11:12 com.apple.mobilesafari/
drwxr-xr-x 2 mobile mobile 102 Mar 18 10:07 com.bitesms/
drwxr-xr-x 2 mobile mobile 102 Apr 15  2013 com.fuyuchi.flexapp/
drwxr-xr-x 2 mobile mobile 102 Nov 19 16:28 libactivator/
Seaslave:/User/Library/Caches/Snapshots root# _
```



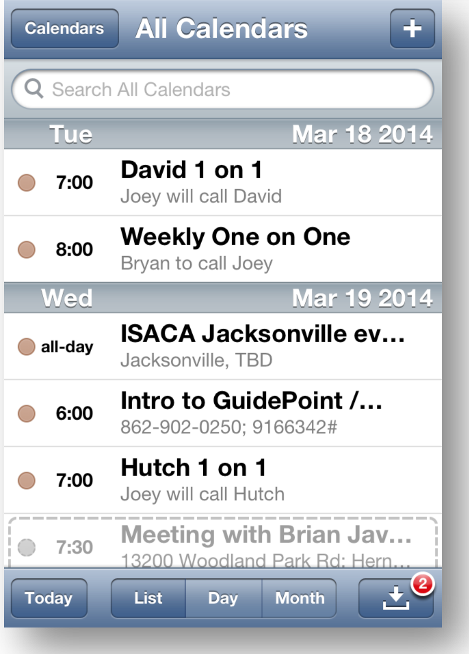
Adrian Mefford

9:59:03 The cup you used was rinsed 😉

Haha ok. Thanks. I guess I just wasn't awake enough to remember. 9:59:55

10:00:20 Np

Text Message



All Calendars

Tue Mar 18 2014

7:00 David 1 on 1
Joey will call David

8:00 Weekly One on One
Bryan to call Joey

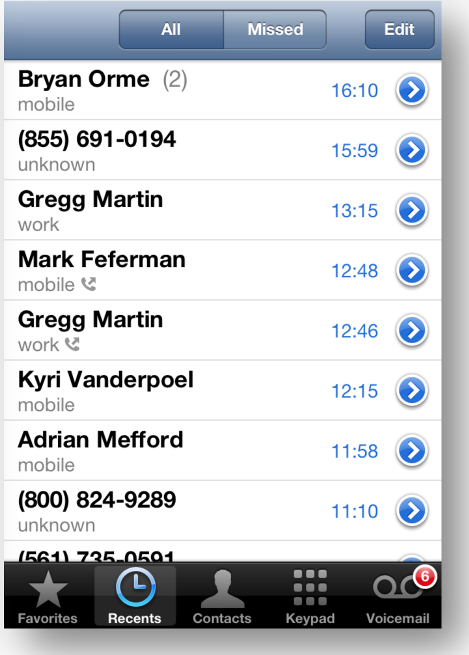
Wed Mar 19 2014

all-day ISACA Jacksonville ev…
Jacksonville, TBD

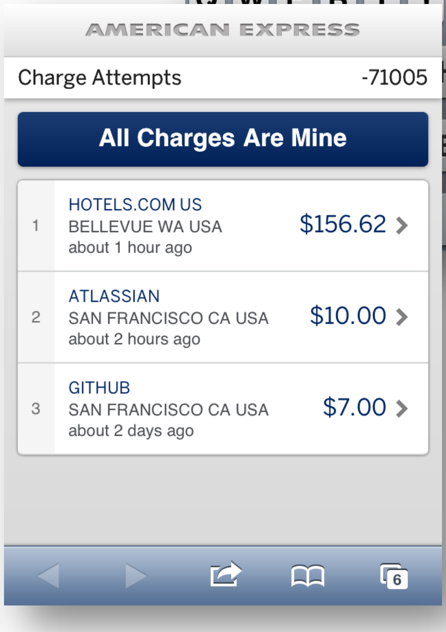
6:00 Intro to GuidePoint /…
862-902-0250; 9166342#

7:00 Hutch 1 on 1
Joey will call Hutch

7:30 Meeting with Brian Jav…
13200 Woodland Park Rd; Hern…



Bryan Orme (2) mobile	16:10
(855) 691-0194 unknown	15:59
Gregg Martin work	13:15
Mark Feferman mobile	12:48
Gregg Martin work	12:46
Kyri Vanderpoel mobile	12:15
Adrian Mefford mobile	11:58
(800) 824-9289 unknown	11:10
(561) 735-0591	

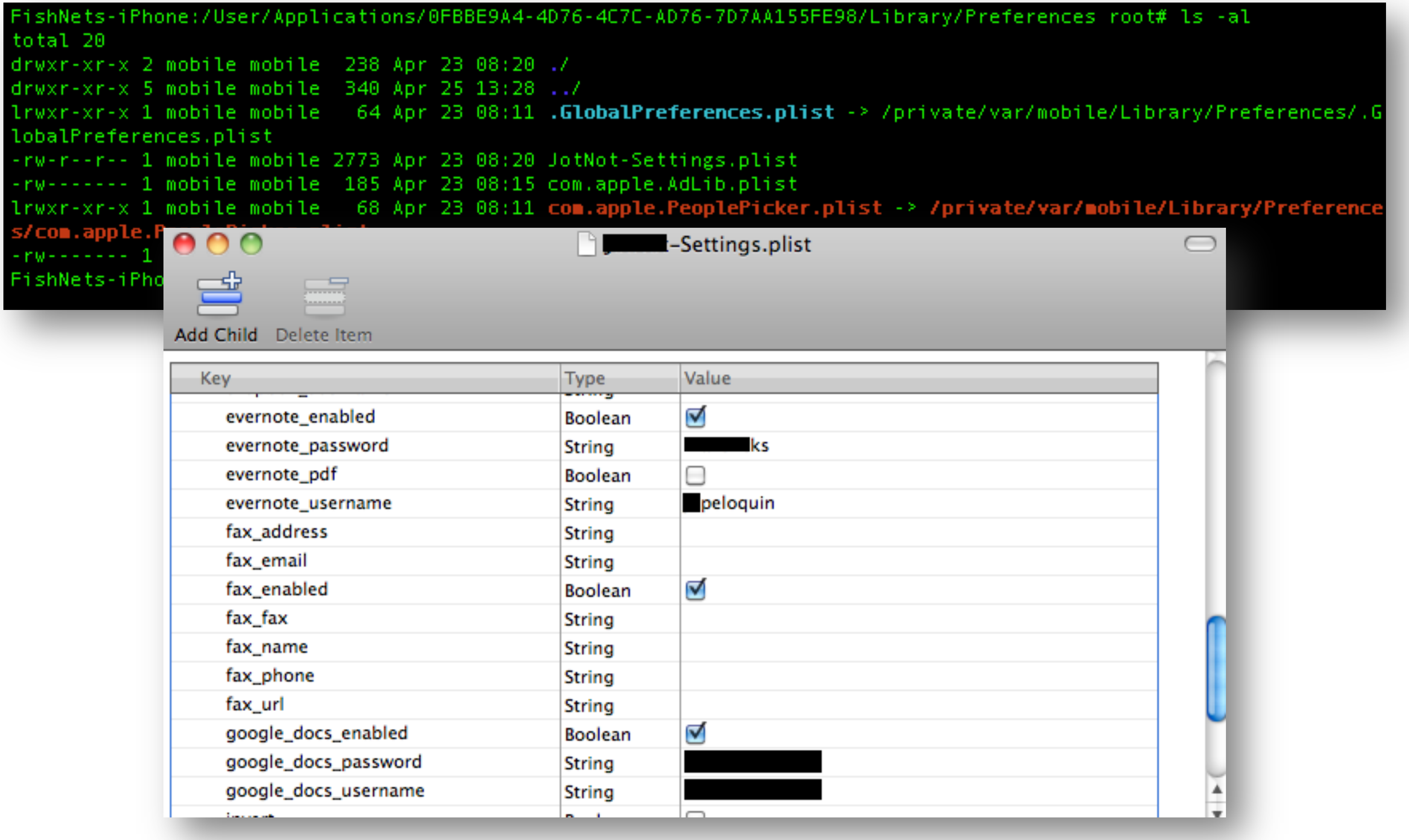


Charge Attempts -71005

All Charges Are Mine

1	HOTELS.COM US BELLEVUE WA USA about 1 hour ago	$156.62
2	ATLASSIAN SAN FRANCISCO CA USA about 2 hours ago	$10.00
3	GITHUB SAN FRANCISCO CA USA about 2 days ago	$7.00

XPENSE MGMT APP

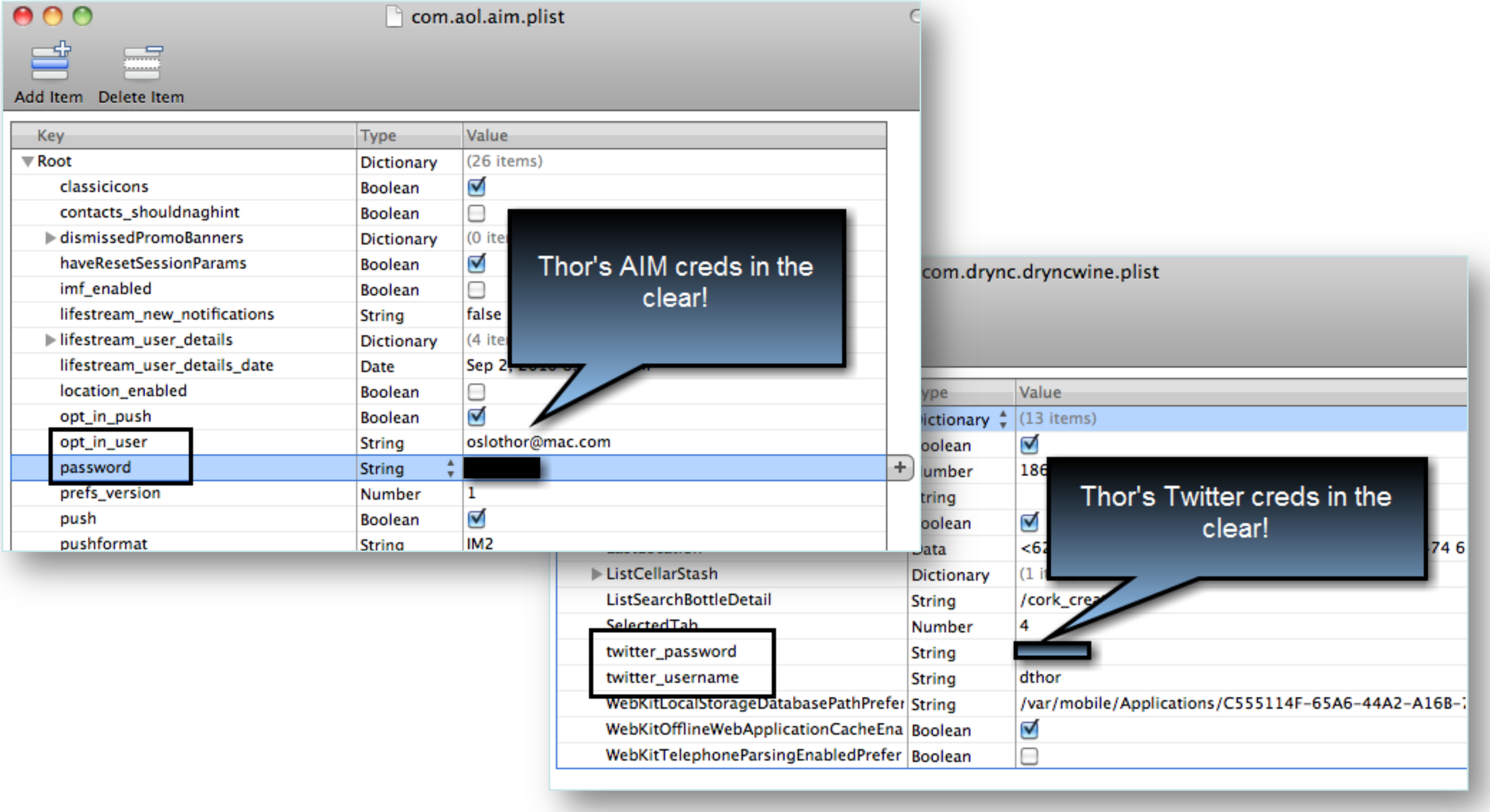


```
FishNets-iPhone:/User/Applications/0FBBE9A4-4D76-4C7C-AD76-7D7AA155FE98/Library/Preferences root# ls -al
total 20
drwxr-xr-x 2 mobile mobile  238 Apr 23 08:20 ./
drwxr-xr-x 5 mobile mobile  340 Apr 25 13:28 ../
lrwxr-xr-x 1 mobile mobile   64 Apr 23 08:11 .GlobalPreferences.plist -> /private/var/mobile/Library/Preferences/.G
lobalPreferences.plist
-rw-r--r-- 1 mobile mobile 2773 Apr 23 08:20 JotNot-Settings.plist
-rw------- 1 mobile mobile  185 Apr 23 08:15 com.apple.AdLib.plist
lrwxr-xr-x 1 mobile mobile   68 Apr 23 08:11 com.apple.PeoplePicker.plist -> /private/var/mobile/Library/Preference
s/com.apple.P
-rw------- 1
FishNets-iPho
```

[redacted]-Settings.plist

Key	Type	Value
evernote_enabled	Boolean	☑
evernote_password	String	[redacted]ks
evernote_pdf	Boolean	☐
evernote_username	String	[redacted]peloquin
fax_address	String	
fax_email	String	
fax_enabled	Boolean	☑
fax_fax	String	
fax_name	String	
fax_phone	String	
fax_url	String	
google_docs_enabled	Boolean	☑
google_docs_password	String	[redacted]
google_docs_username	String	[redacted]

CHAT / SOCIAL APPS



com.aol.aim.plist

Key	Type	Value
Root	Dictionary	(26 items)
classicicons	Boolean	☑
contacts_shouldnaghint	Boolean	□
dismissedPromoBanners	Dictionary	(0 ite
haveResetSessionParams	Boolean	☑
imf_enabled	Boolean	□
lifestream_new_notifications	String	false
lifestream_user_details	Dictionary	(4 ite
lifestream_user_details_date	Date	Sep 2
location_enabled	Boolean	□
opt_in_push	Boolean	☑
opt_in_user	String	oslothor@mac.com
password	String	[redacted]
prefs_version	Number	1
push	Boolean	☑
pushformat	String	IM2

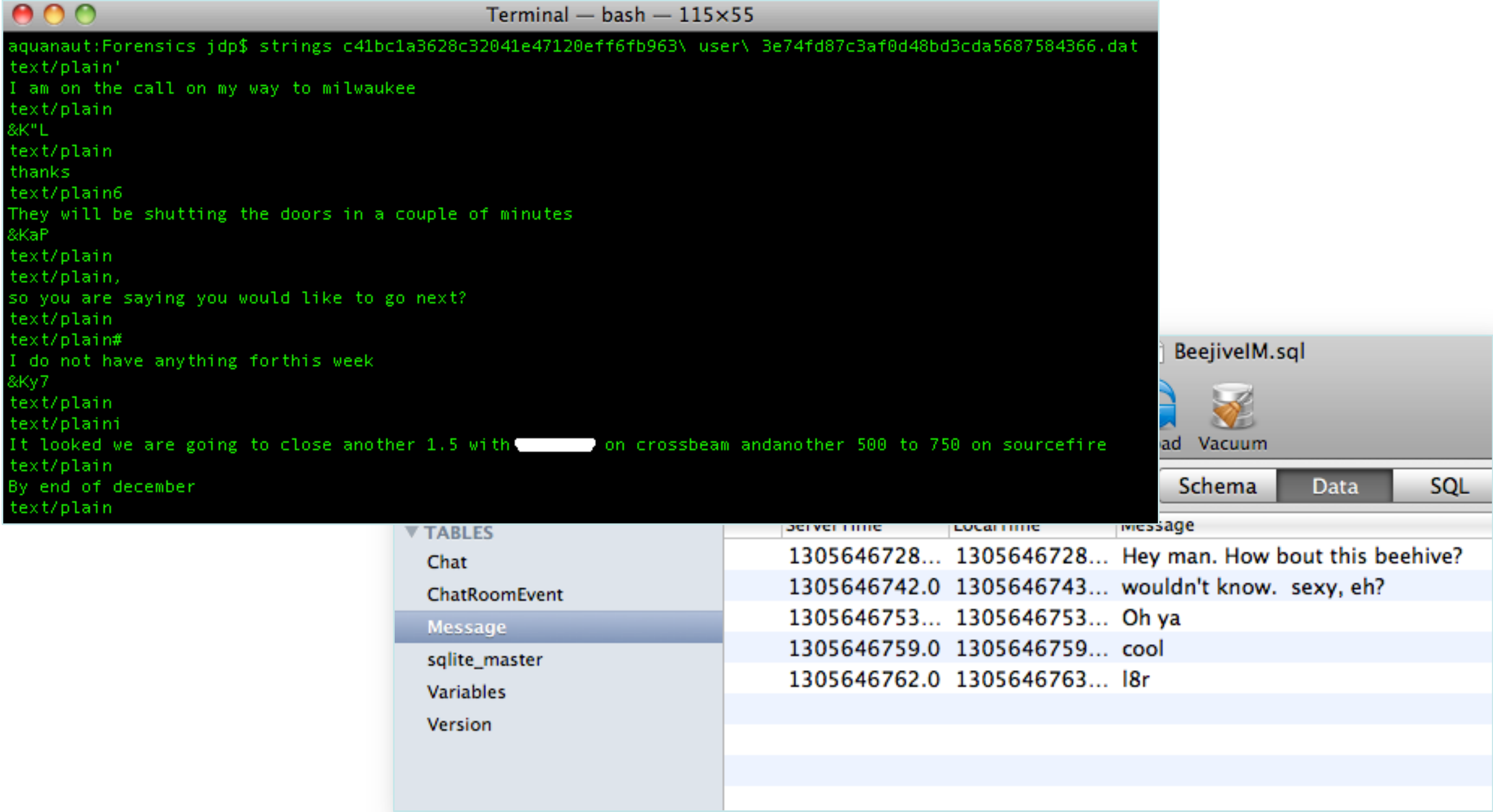
Thor's AIM creds in the clear!

com.drync.dryncwine.plist

	ype	Value
	ictionary	(13 items)
	oolean	☑
	umber	186
	tring	
	oolean	☑
	ata	<62
ListCellarStash	Dictionary	(1 i
ListSearchBottleDetail	String	/cork_cre
SelectedTab	Number	4
twitter_password	String	[redacted]
twitter_username	String	dthor
WebKitLocalStorageDatabasePathPrefer	String	/var/mobile/Applications/C555114F-65A6-44A2-A16B-
WebKitOfflineWebApplicationCacheEna	Boolean	☑
WebKitTelephoneParsingEnabledPrefer	Boolean	□

Thor's Twitter creds in the clear!

CHAT / SOCIAL APPS



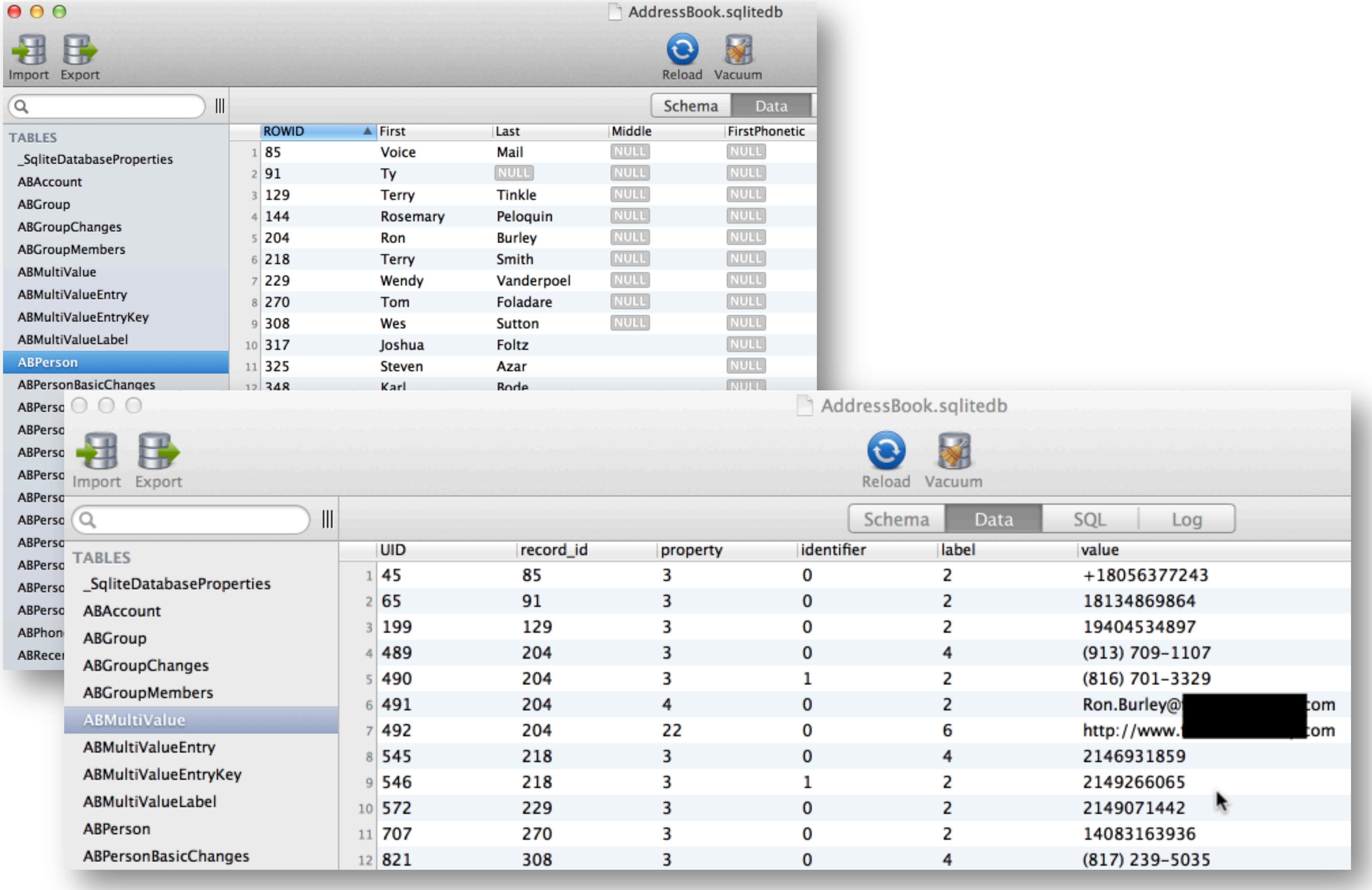
```
aquanaut:Forensics jdp$ strings c41bc1a3628c32041e47120eff6fb963\ user\ 3e74fd87c3af0d48bd3cda5687584366.dat
text/plain'
I am on the call on my way to milwaukee
text/plain
&K"L
text/plain
thanks
text/plain6
They will be shutting the doors in a couple of minutes
&KaP
text/plain
text/plain,
so you are saying you would like to go next?
text/plain
text/plain#
I do not have anything forthis week
&Ky7
text/plain
text/plaini
It looked we are going to close another 1.5 with [redacted] on crossbeam andanother 500 to 750 on sourcefire
text/plain
By end of december
text/plain
```

TABLES

- Chat
- ChatRoomEvent
- Message
- sqlite_master
- Variables
- Version

Server Time	Local Time	Message
1305646728...	1305646728...	Hey man. How bout this beehive?
1305646742.0	1305646743...	wouldn't know. sexy, eh?
1305646753...	1305646753...	Oh ya
1305646759.0	1305646759...	cool
1305646762.0	1305646763...	l8r

CONTACTS



TABLES

- _SqliteDatabaseProperties
- ABAccount
- ABGroup
- ABGroupChanges
- ABGroupMembers
- ABMultiValue
- ABMultiValueEntry
- ABMultiValueEntryKey
- ABMultiValueLabel
- ABPerson
- ABPersonBasicChanges
- ABPerso
- ABPerso
- ABPerso
- ABPerso
- ABPerso
- ABPerso
- ABPerso
- ABPerso
- ABPerso
- ABPerso
- ABPhon
- ABRecer

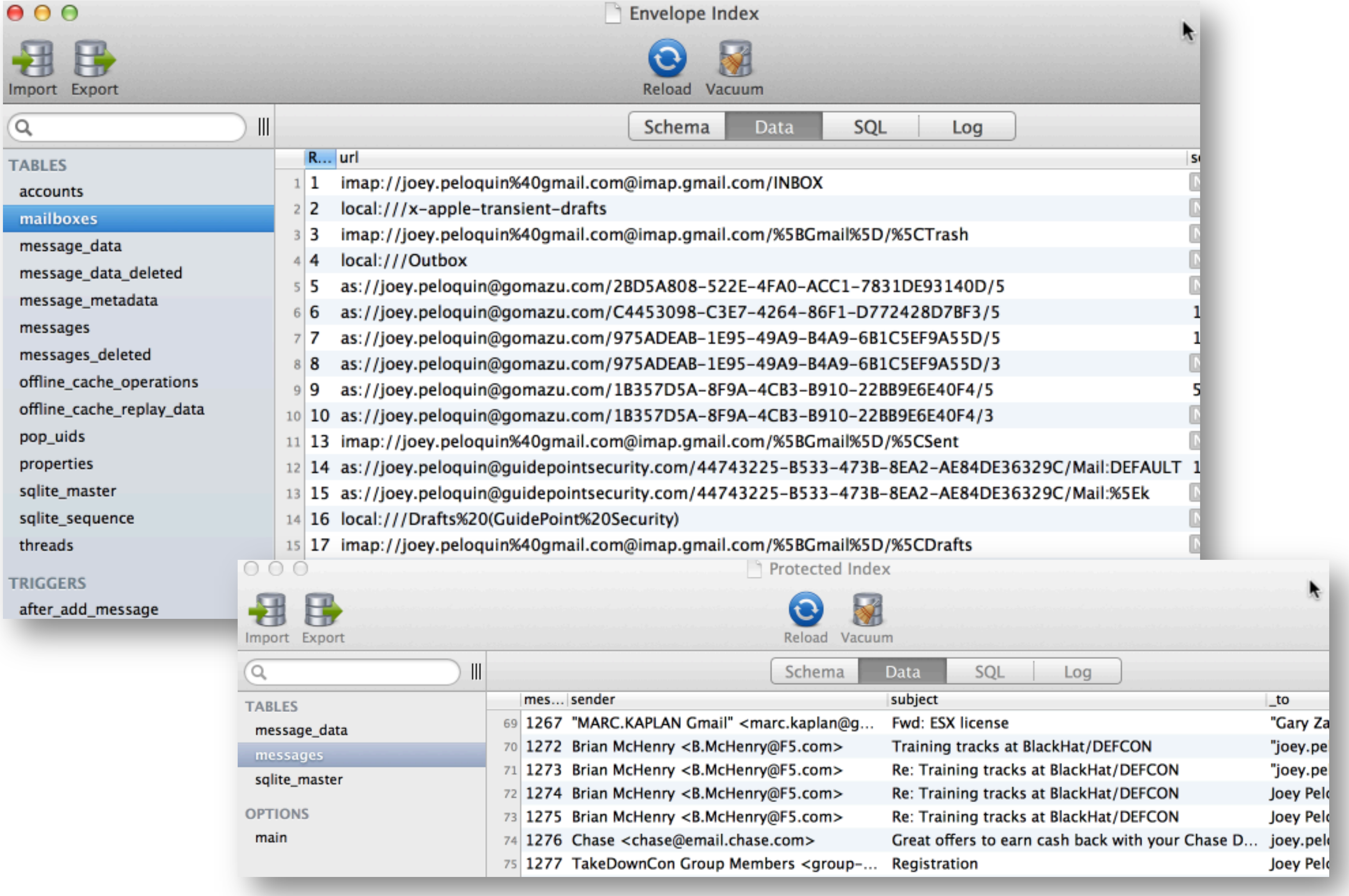
ROWID	First	Last	Middle	FirstPhonetic
85	Voice	Mail	NULL	NULL
91	Ty	NULL	NULL	NULL
129	Terry	Tinkle	NULL	NULL
144	Rosemary	Peloquin	NULL	NULL
204	Ron	Burley	NULL	NULL
218	Terry	Smith	NULL	NULL
229	Wendy	Vanderpoel	NULL	NULL
270	Tom	Foladare	NULL	NULL
308	Wes	Sutton	NULL	NULL
317	Joshua	Foltz		NULL
325	Steven	Azar		NULL
348	Karl	Bode		NULL

TABLES

- _SqliteDatabaseProperties
- ABAccount
- ABGroup
- ABGroupChanges
- ABGroupMembers
- ABMultiValue
- ABMultiValueEntry
- ABMultiValueEntryKey
- ABMultiValueLabel
- ABPerson
- ABPersonBasicChanges

UID	record_id	property	identifier	label	value
45	85	3	0	2	+18056377243
65	91	3	0	2	18134869864
199	129	3	0	2	19404534897
489	204	3	0	4	(913) 709-1107
490	204	3	1	2	(816) 701-3329
491	204	4	0	2	Ron.Burley@[redacted]om
492	204	22	0	6	http://www.[redacted]om
545	218	3	0	4	2146931859
546	218	3	1	2	2149266065
572	229	3	0	2	2149071442
707	270	3	0	2	14083163936
821	308	3	0	4	(817) 239-5035

MAIL



TABLES
- accounts
- mailboxes
- message_data
- message_data_deleted
- message_metadata
- messages
- messages_deleted
- offline_cache_operations
- offline_cache_replay_data
- pop_uids
- properties
- sqlite_master
- sqlite_sequence
- threads

TRIGGERS
- after_add_message

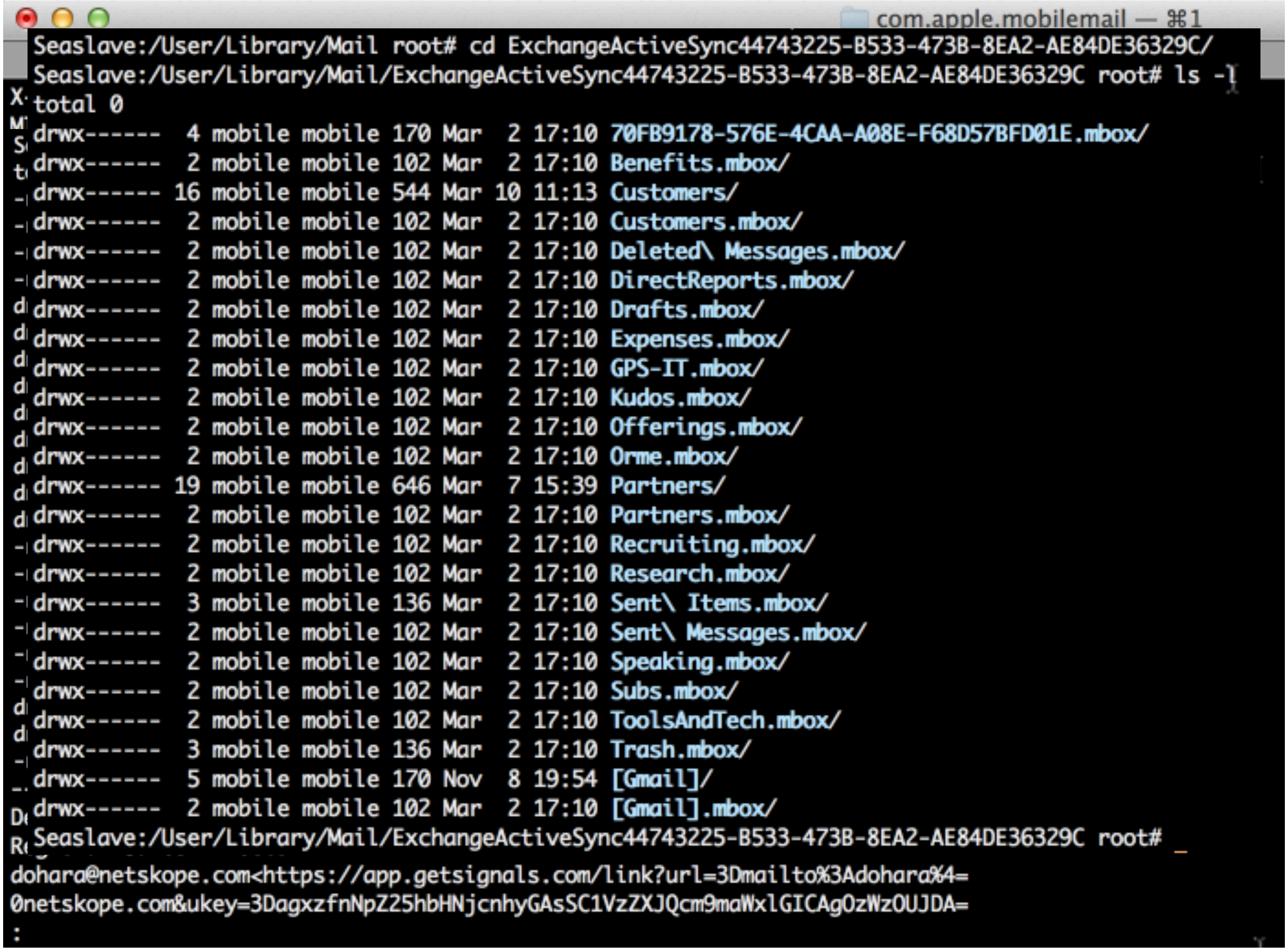
	R...	url	s
1	1	imap://joey.peloquin%40gmail.com@imap.gmail.com/INBOX	
2	2	local:///x-apple-transient-drafts	
3	3	imap://joey.peloquin%40gmail.com@imap.gmail.com/%5BGmail%5D/%5CTrash	
4	4	local:///Outbox	
5	5	as://joey.peloquin@gomazu.com/2BD5A808-522E-4FA0-ACC1-7831DE93140D/5	
6	6	as://joey.peloquin@gomazu.com/C4453098-C3E7-4264-86F1-D772428D7BF3/5	1
7	7	as://joey.peloquin@gomazu.com/975ADEAB-1E95-49A9-B4A9-6B1C5EF9A55D/5	1
8	8	as://joey.peloquin@gomazu.com/975ADEAB-1E95-49A9-B4A9-6B1C5EF9A55D/3	
9	9	as://joey.peloquin@gomazu.com/1B357D5A-8F9A-4CB3-B910-22BB9E6E40F4/5	5
10	10	as://joey.peloquin@gomazu.com/1B357D5A-8F9A-4CB3-B910-22BB9E6E40F4/3	
11	13	imap://joey.peloquin%40gmail.com@imap.gmail.com/%5BGmail%5D/%5CSent	
12	14	as://joey.peloquin@guidepointsecurity.com/44743225-B533-473B-8EA2-AE84DE36329C/Mail:DEFAULT	1
13	15	as://joey.peloquin@guidepointsecurity.com/44743225-B533-473B-8EA2-AE84DE36329C/Mail:%5Ek	
14	16	local:///Drafts%20(GuidePoint%20Security)	
15	17	imap://joey.peloquin%40gmail.com@imap.gmail.com/%5BGmail%5D/%5CDrafts	

TABLES
- message_data
- messages
- sqlite_master

OPTIONS
- main

	mes...	sender	subject	_to
69	1267	"MARC.KAPLAN Gmail" <marc.kaplan@g...	Fwd: ESX license	"Gary Za
70	1272	Brian McHenry <B.McHenry@F5.com>	Training tracks at BlackHat/DEFCON	"joey.pe
71	1273	Brian McHenry <B.McHenry@F5.com>	Re: Training tracks at BlackHat/DEFCON	"joey.pe
72	1274	Brian McHenry <B.McHenry@F5.com>	Re: Training tracks at BlackHat/DEFCON	Joey Pelo
73	1275	Brian McHenry <B.McHenry@F5.com>	Re: Training tracks at BlackHat/DEFCON	Joey Pelo
74	1276	Chase <chase@email.chase.com>	Great offers to earn cash back with your Chase D...	joey.pelo
75	1277	TakeDownCon Group Members <group-...	Registration	Joey Pelo

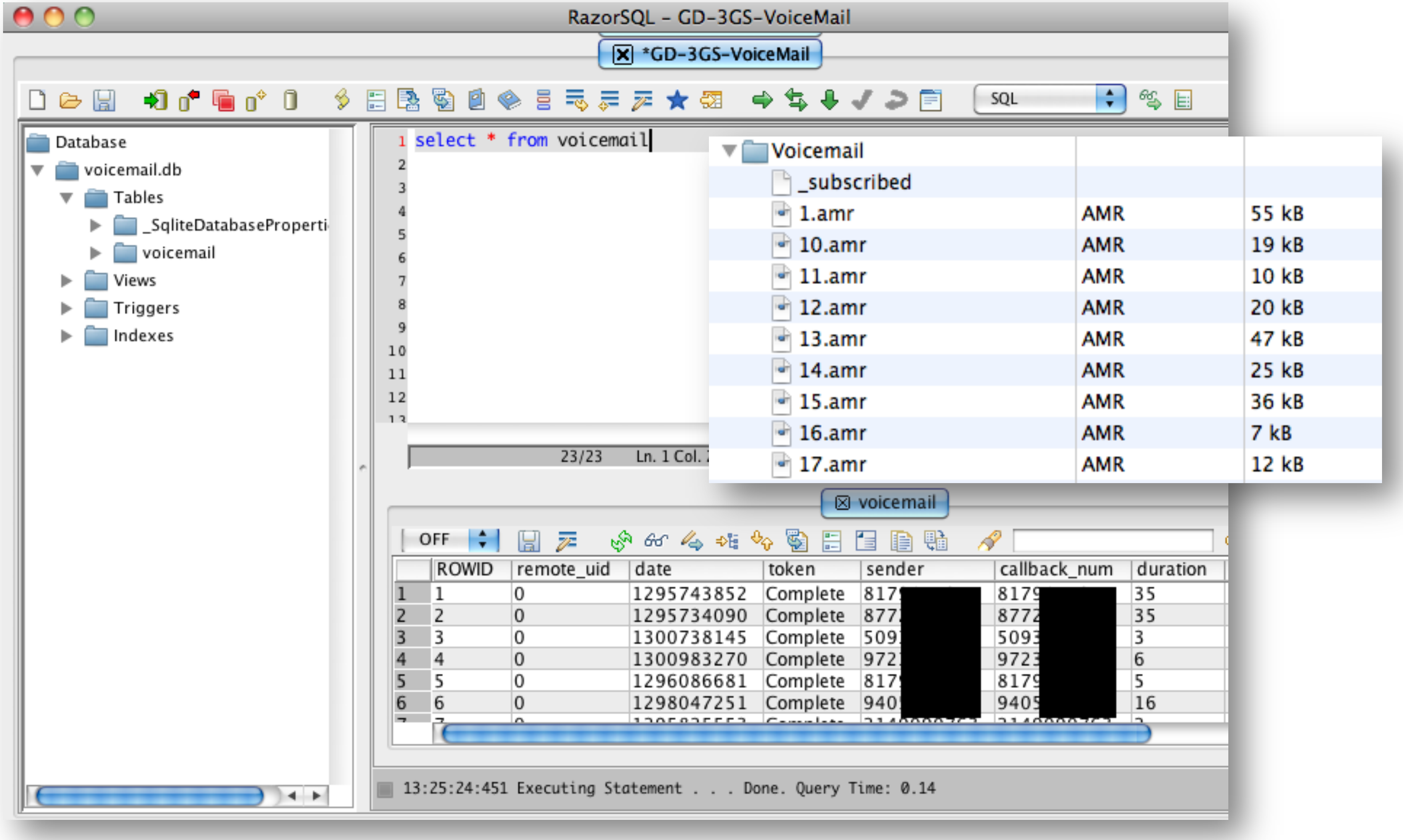
MO' MAIL



```
Seaslave:/User/Library/Mail root# cd ExchangeActiveSync44743225-B533-473B-8EA2-AE84DE36329C/
Seaslave:/User/Library/Mail/ExchangeActiveSync44743225-B533-473B-8EA2-AE84DE36329C root# ls -l
total 0
drwx------  4 mobile mobile 170 Mar  2 17:10 70FB9178-576E-4CAA-A08E-F68D57BFD01E.mbox/
drwx------  2 mobile mobile 102 Mar  2 17:10 Benefits.mbox/
drwx------ 16 mobile mobile 544 Mar 10 11:13 Customers/
drwx------  2 mobile mobile 102 Mar  2 17:10 Customers.mbox/
drwx------  2 mobile mobile 102 Mar  2 17:10 Deleted\ Messages.mbox/
drwx------  2 mobile mobile 102 Mar  2 17:10 DirectReports.mbox/
drwx------  2 mobile mobile 102 Mar  2 17:10 Drafts.mbox/
drwx------  2 mobile mobile 102 Mar  2 17:10 Expenses.mbox/
drwx------  2 mobile mobile 102 Mar  2 17:10 GPS-IT.mbox/
drwx------  2 mobile mobile 102 Mar  2 17:10 Kudos.mbox/
drwx------  2 mobile mobile 102 Mar  2 17:10 Offerings.mbox/
drwx------  2 mobile mobile 102 Mar  2 17:10 Orme.mbox/
drwx------ 19 mobile mobile 646 Mar  7 15:39 Partners/
drwx------  2 mobile mobile 102 Mar  2 17:10 Partners.mbox/
drwx------  2 mobile mobile 102 Mar  2 17:10 Recruiting.mbox/
drwx------  2 mobile mobile 102 Mar  2 17:10 Research.mbox/
drwx------  3 mobile mobile 136 Mar  2 17:10 Sent\ Items.mbox/
drwx------  2 mobile mobile 102 Mar  2 17:10 Sent\ Messages.mbox/
drwx------  2 mobile mobile 102 Mar  2 17:10 Speaking.mbox/
drwx------  2 mobile mobile 102 Mar  2 17:10 Subs.mbox/
drwx------  2 mobile mobile 102 Mar  2 17:10 ToolsAndTech.mbox/
drwx------  3 mobile mobile 136 Mar  2 17:10 Trash.mbox/
drwx------  5 mobile mobile 170 Nov  8 19:54 [Gmail]/
drwx------  2 mobile mobile 102 Mar  2 17:10 [Gmail].mbox/
Seaslave:/User/Library/Mail/ExchangeActiveSync44743225-B533-473B-8EA2-AE84DE36329C root# _
dohara@netskope.com<https://app.getsignals.com/link?url=3Dmailto%3Adohara%4=
0netskope.com&ukey=3DagxzfnNpZ25hbHNjcnhyGAsSC1VzZXJQcm9maWxlGICAg0zWz0UJDA=
:
```

DEMO!

VOICEMAIL



RazorSQL - GD-3GS-VoiceMail

*GD-3GS-VoiceMail

- Database
  - voicemail.db
    - Tables
      - _SqliteDatabaseProperti
      - voicemail
    - Views
    - Triggers
    - Indexes

```
select * from voicemail
```

23/23 Ln. 1 Col.

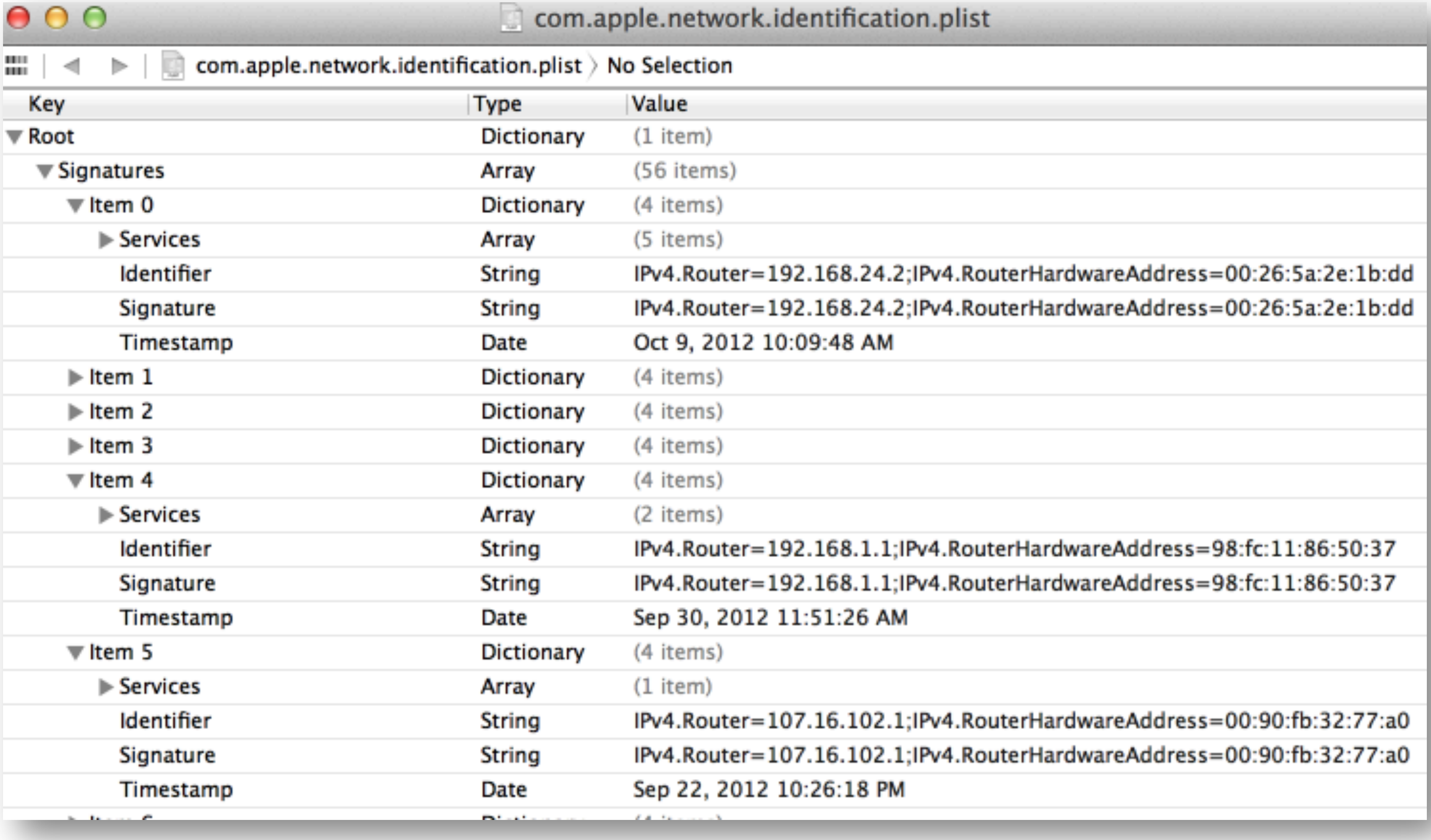
Voicemail		
_subscribed		
1.amr	AMR	55 kB
10.amr	AMR	19 kB
11.amr	AMR	10 kB
12.amr	AMR	20 kB
13.amr	AMR	47 kB
14.amr	AMR	25 kB
15.amr	AMR	36 kB
16.amr	AMR	7 kB
17.amr	AMR	12 kB

voicemail

	ROWID	remote_uid	date	token	sender	callback_num	duration
1	1	0	1295743852	Complete	[redacted]	[redacted]	35
2	2	0	1295734090	Complete	[redacted]	[redacted]	35
3	3	0	1300738145	Complete	[redacted]	[redacted]	3
4	4	0	1300983270	Complete	[redacted]	[redacted]	6
5	5	0	1296086681	Complete	[redacted]	[redacted]	5
6	6	0	1298047251	Complete	[redacted]	[redacted]	16

```
13:25:24:451 Executing Statement . . . Done. Query Time: 0.14
```

NETWORK CONFIG

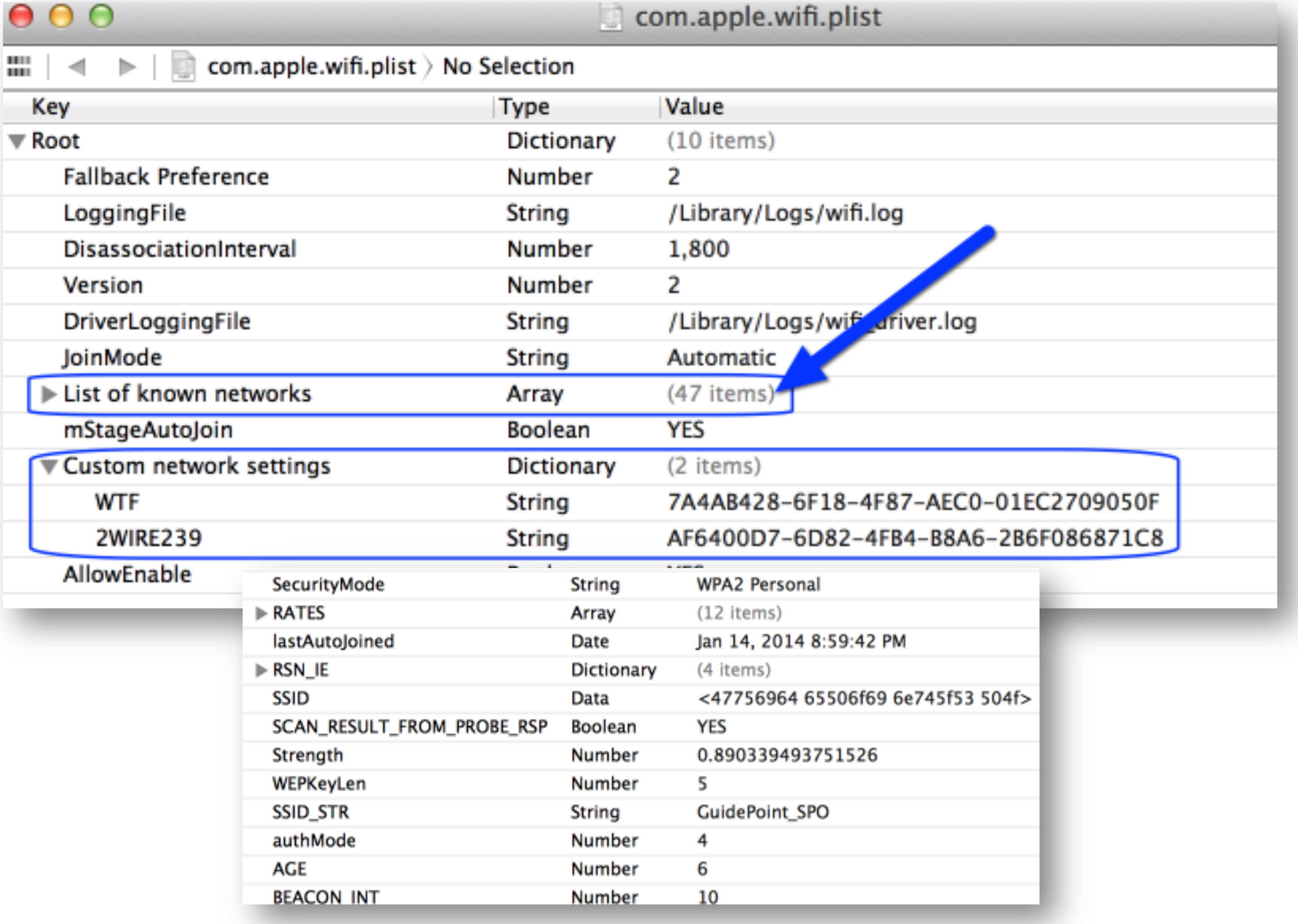


com.apple.network.identification.plist

com.apple.network.identification.plist 〉 No Selection

Key	Type	Value
▼ Root	Dictionary	(1 item)
▼ Signatures	Array	(56 items)
▼ Item 0	Dictionary	(4 items)
▶ Services	Array	(5 items)
Identifier	String	IPv4.Router=192.168.24.2;IPv4.RouterHardwareAddress=00:26:5a:2e:1b:dd
Signature	String	IPv4.Router=192.168.24.2;IPv4.RouterHardwareAddress=00:26:5a:2e:1b:dd
Timestamp	Date	Oct 9, 2012 10:09:48 AM
▶ Item 1	Dictionary	(4 items)
▶ Item 2	Dictionary	(4 items)
▶ Item 3	Dictionary	(4 items)
▼ Item 4	Dictionary	(4 items)
▶ Services	Array	(2 items)
Identifier	String	IPv4.Router=192.168.1.1;IPv4.RouterHardwareAddress=98:fc:11:86:50:37
Signature	String	IPv4.Router=192.168.1.1;IPv4.RouterHardwareAddress=98:fc:11:86:50:37
Timestamp	Date	Sep 30, 2012 11:51:26 AM
▼ Item 5	Dictionary	(4 items)
▶ Services	Array	(1 item)
Identifier	String	IPv4.Router=107.16.102.1;IPv4.RouterHardwareAddress=00:90:fb:32:77:a0
Signature	String	IPv4.Router=107.16.102.1;IPv4.RouterHardwareAddress=00:90:fb:32:77:a0
Timestamp	Date	Sep 22, 2012 10:26:18 PM
▶ Item 6	Dictionary	(4 items)

WIFI CONFIG



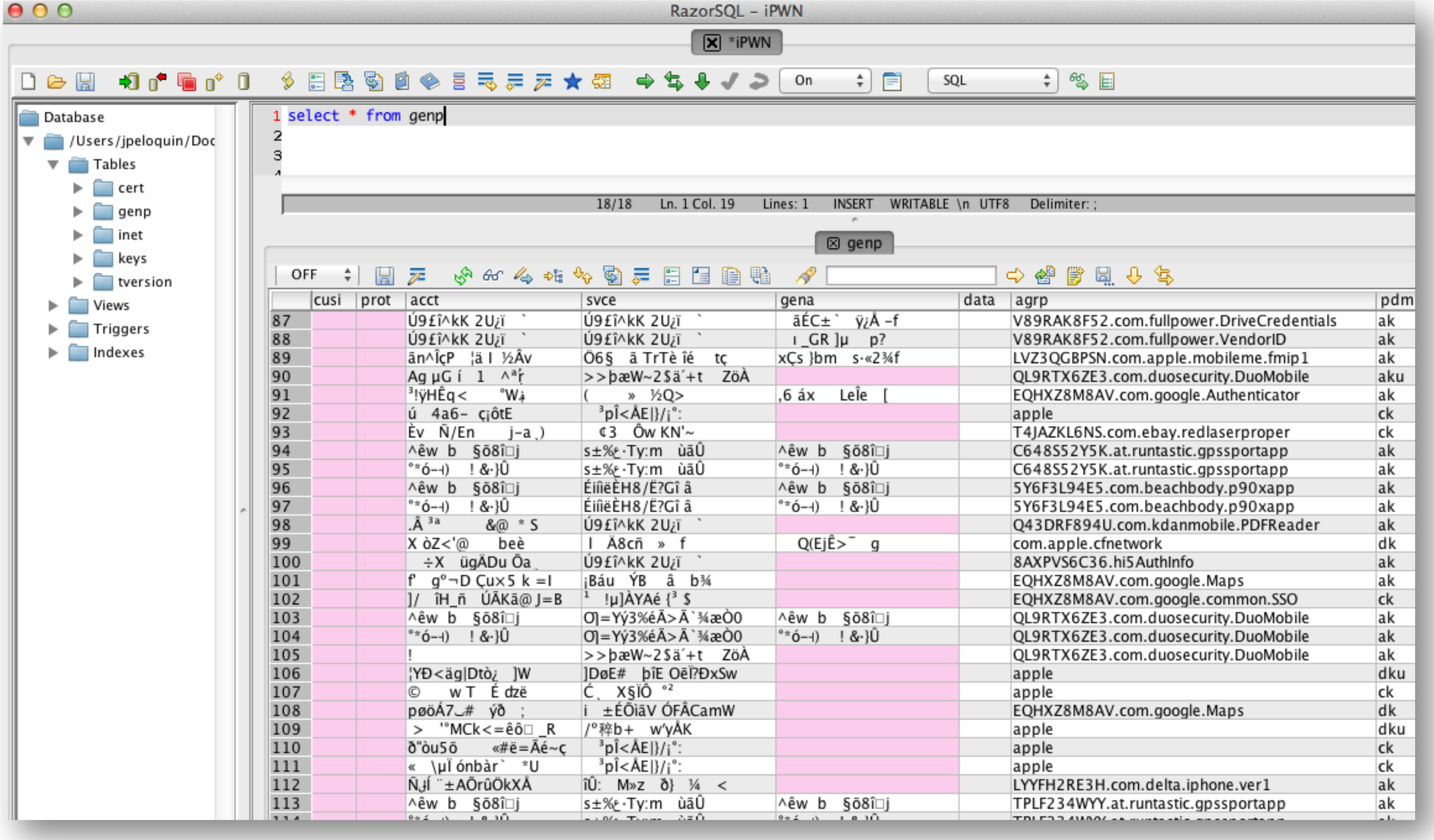
com.apple.wifi.plist

com.apple.wifi.plist 〉 No Selection

Key	Type	Value
▼ Root	Dictionary	(10 items)
Fallback Preference	Number	2
LoggingFile	String	/Library/Logs/wifi.log
DisassociationInterval	Number	1,800
Version	Number	2
DriverLoggingFile	String	/Library/Logs/wifi_driver.log
JoinMode	String	Automatic
▶ List of known networks	Array	(47 items)
mStageAutoJoin	Boolean	YES
▼ Custom network settings	Dictionary	(2 items)
WTF	String	7A4AB428-6F18-4F87-AEC0-01EC2709050F
2WIRE239	String	AF6400D7-6D82-4FB4-B8A6-2B6F086871C8
AllowEnable	Boolean	YES

SecurityMode	String	WPA2 Personal
▶ RATES	Array	(12 items)
lastAutoJoined	Date	Jan 14, 2014 8:59:42 PM
▶ RSN_IE	Dictionary	(4 items)
SSID	Data	<47756964 65506f69 6e745f53 504f>
SCAN_RESULT_FROM_PROBE_RSP	Boolean	YES
Strength	Number	0.890339493751526
WEPKeyLen	Number	5
SSID_STR	String	GuidePoint_SPO
authMode	Number	4
AGE	Number	6
BEACON_INT	Number	10

KEYCHAIN

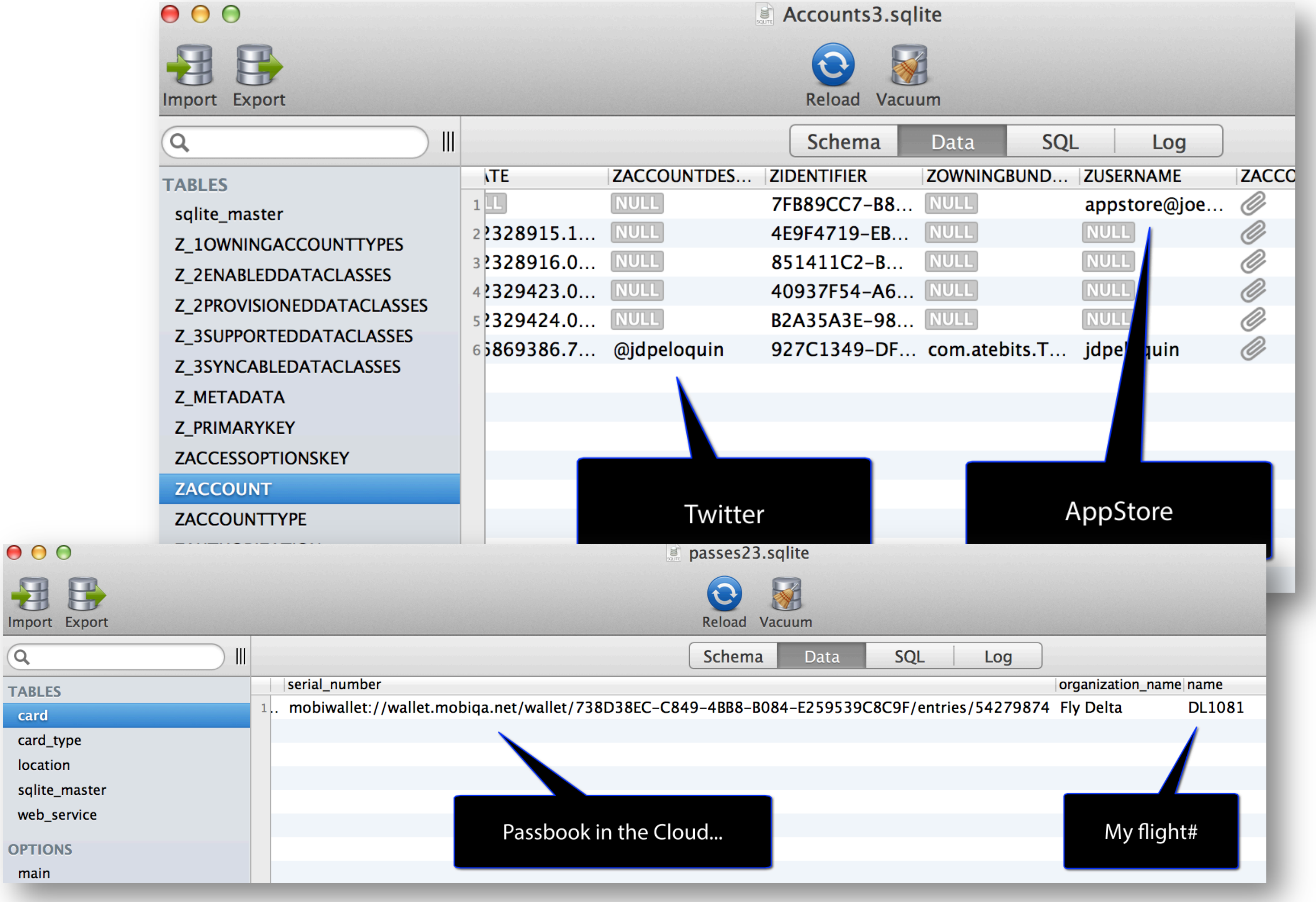


```
select * from genp
```

```
18/18     Ln. 1 Col. 19     Lines: 1     INSERT   WRITABLE  \n   UTF8     Delimiter: ;
```

	cusi	prot	acct	svce	gena	data	agrp	pdm
87			Ú9£î^kK 2U¿ï `	Ú9£î^kK 2U¿ï `	ãÉC± ` ÿ¿Å -f		V89RAK8F52.com.fullpower.DriveCredentials	ak
88			Ú9£î^kK 2U¿ï `	Ú9£î^kK 2U¿ï `	ı _GR]µ p?		V89RAK8F52.com.fullpower.VendorID	ak
89			ãn^ÎçP ¦ä I ½Âv	Ö6§ ã TrTè îé tç	xÇs }bm s·«2¾f		LVZ3QGBPSN.com.apple.mobileme.fmip1	ak
90			Ag µG í 1 ^ªŗ	>>þæW~2$ä´+t ZöÀ			QL9RTX6ZE3.com.duosecurity.DuoMobile	aku
91			³!ÿHÊq< °W¡	(» ½Q>	,6 áx LeÎe [		EQHXZ8M8AV.com.google.Authenticator	ak
92			ú 4a6- ç¡ôtE	³pÎ<ÅE|}/¡°:			apple	ck
93			Èv Ñ/En j-a ̧)	¢3 Ôw KN'~			T4JAZKL6NS.com.ebay.redlaserproper	ck
94			^êw b §õ8î□j	s±%ț·Ty:m ùãÛ	^êw b §õ8î□j		C648S52Y5K.at.runtastic.gpssportapp	ak
95			°*ó–ı) ! &·}Û	s±%ț·Ty:m ùãÛ	°*ó–ı) ! &·}Û		C648S52Y5K.at.runtastic.gpssportapp	ak
96			^êw b §õ8î□j	ÉiîïëÈH8/Ë?Gî â	^êw b §õ8î□j		5Y6F3L94E5.com.beachbody.p90xapp	ak
97			°*ó–ı) ! &·}Û	ÉiîïëÈH8/Ë?Gî â	°*ó–ı) ! &·}Û		5Y6F3L94E5.com.beachbody.p90xapp	ak
98			.Â ³ª &@ * S	Ú9£î^kK 2U¿ï `			Q43DRF894U.com.kdanmobile.PDFReader	ak
99			X òZ<'@ beè	I Ä8cñ » f	Q(EjÊ>¯ g		com.apple.cfnetwork	dk
100			÷X ügÄDu Õa ̤	Ú9£î^kK 2U¿ï `			8AXPVS6C36.hi5AuthInfo	ak
101			f' g°¬D Çu×5 k =I	¡Báu ÝB â b¾			EQHXZ8M8AV.com.google.Maps	ak
102			]/ îH_ñ ÚÃKã@ J=B	¹ !µ]ÀYAé {³ $			EQHXZ8M8AV.com.google.common.SSO	ck
103			^êw b §õ8î□j	Ơ]=Yý3%éÃ>Ã`¾æÒ0	^êw b §õ8î□j		QL9RTX6ZE3.com.duosecurity.DuoMobile	ak
104			°*ó–ı) ! &·}Û	Ơ]=Yý3%éÃ>Ã`¾æÒ0	°*ó–ı) ! &·}Û		QL9RTX6ZE3.com.duosecurity.DuoMobile	ak
105			!	>>þæW~2$ä´+t ZöÀ			QL9RTX6ZE3.com.duosecurity.DuoMobile	ak
106			¦YÐ<äg|Dtò¿]W	]DøE# þîE OëÏ?ÐxSw			apple	dku
107			© w T É ǳë	Ć ̧ X§ÏÔ °²			apple	ck
108			pøöÁ7‿# ýð ;	i ±ÉÕìãV ÓFÂCamW			EQHXZ8M8AV.com.google.Maps	dk
109			> '°MCk<=êô□ _R	/°粹b+ w'yÅK			apple	dku
110			ð"òu5õ «#ë=Ãé~ç	³pÎ<ÅE|}/¡°:			apple	ck
111			« \µÏ ónbàr` *U	³pÎ<ÅE|}/¡°:			apple	ck
112			Ñ¸í ¨±AÕrûÖkXÅ	îÛ: M»z ð} ¼ <			LYYFH2RE3H.com.delta.iphone.ver1	ak
113			^êw b §õ8î□j	s±%ț·Ty:m ùãÛ	^êw b §õ8î□j		TPLF234WYY.at.runtastic.gpssportapp	ak
114			°*ó–ı) ! &·}Û	s±%ț·Ty:m ùãÛ	°*ó–ı) ! &·}Û		TPLF234WYY.at.runtastic.gpssportapp	ak

PASSBOOK, ACCOUNTS



TABLES
- sqlite_master
- Z_1OWNINGACCOUNTTYPES
- Z_2ENABLEDDATACLASSES
- Z_2PROVISIONEDDATACLASSES
- Z_3SUPPORTEDDATACLASSES
- Z_3SYNCABLEDATACLASSES
- Z_METADATA
- Z_PRIMARYKEY
- ZACCESSOPTIONSKEY
- ZACCOUNT
- ZACCOUNTTYPE

	ATE	ZACCOUNTDES…	ZIDENTIFIER	ZOWNINGBUND…	ZUSERNAME	ZACCO
1	LL	NULL	7FB89CC7-B8…	NULL	appstore@joe…	📎
2	2328915.1…	NULL	4E9F4719-EB…	NULL	NULL	📎
3	2328916.0…	NULL	851411C2-B…	NULL	NULL	📎
4	2329423.0…	NULL	40937F54-A6…	NULL	NULL	📎
5	2329424.0…	NULL	B2A35A3E-98…	NULL	NULL	📎
6	5869386.7…	@jdpeloquin	927C1349-DF…	com.atebits.T…	jdpe quin	📎

Twitter

AppStore

TABLES
- card
- card_type
- location
- sqlite_master
- web_service

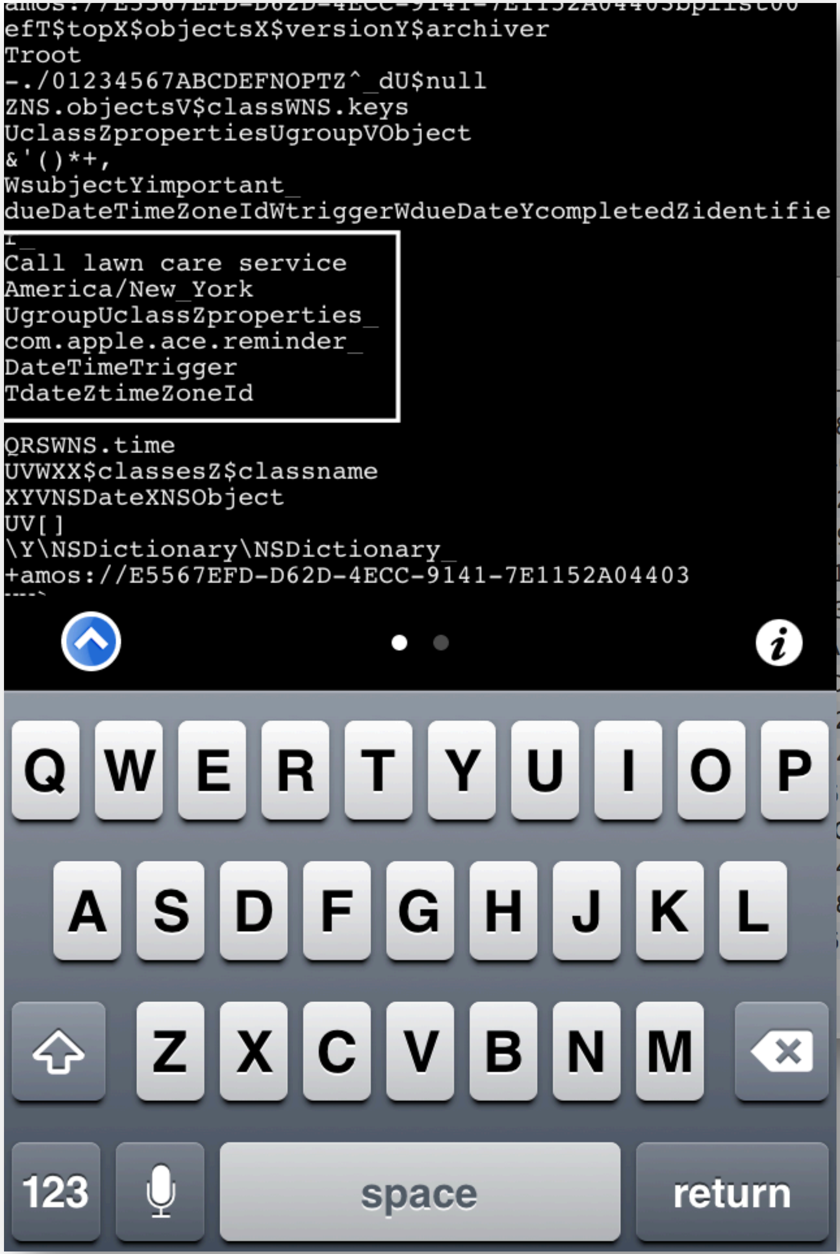
OPTIONS
- main

	serial_number	organization_name	name
1	mobiwallet://wallet.mobiqa.net/wallet/738D38EC-C849-4BB8-B084-E259539C8C9F/entries/54279874	Fly Delta	DL1081

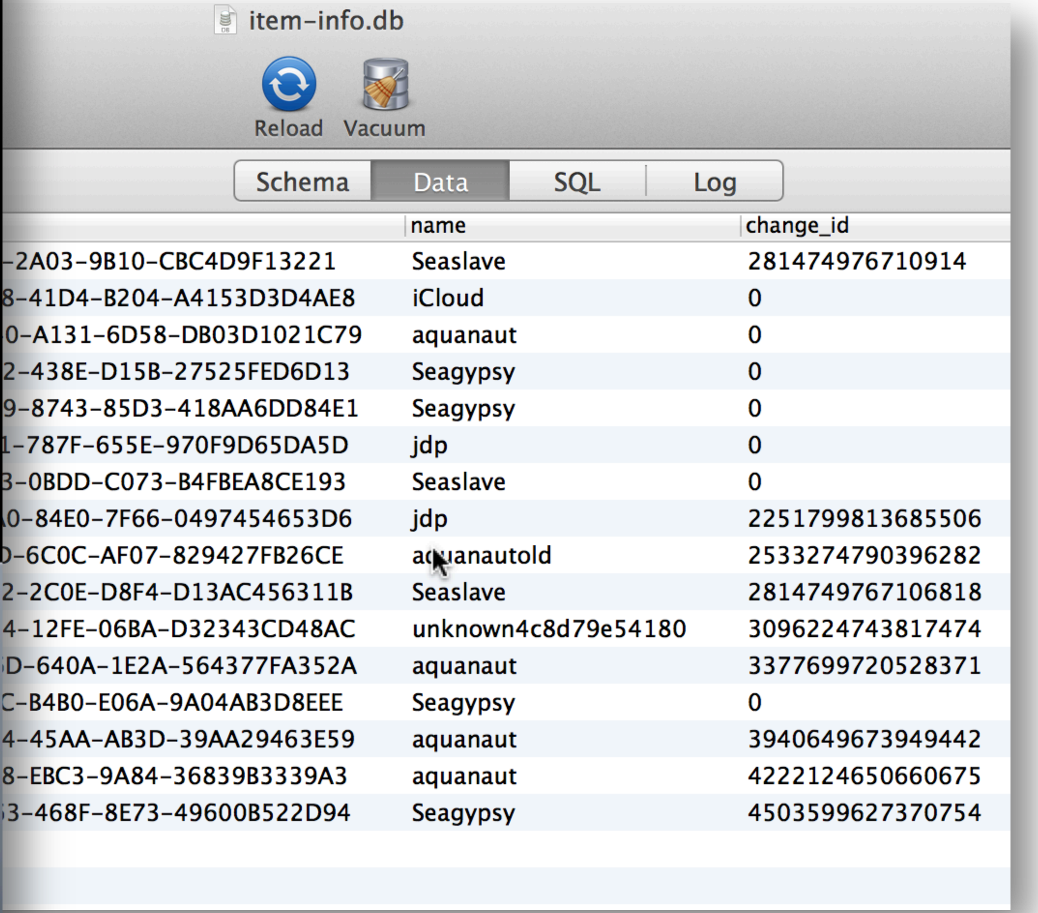
Passbook in the Cloud...

My flight#

UBIQUITY, ASSISTANT



```
amos://E5567EFD-D62D-4ECC-9141-7E1152A04403bplist00
efT$topX$objectsX$versionY$archiver
Troot
-./01234567ABCDEFNOPTZ^_dU$null
ZNS.objectsV$classWNS.keys
UclassZpropertiesUgroupVObject
&'()*+,
WsubjectYimportant_
dueDateTimeZoneIdWtriggerWdueDateYcompletedZidentifie
r_
Call lawn care service
America/New_York
UgroupUclassZproperties_
com.apple.ace.reminder_
DateTimeTrigger
TdateZtimeZoneId

QRSWNS.time
UVWXX$classesZ$classname
XYVNSDateXNSObject
UV[]
\Y\NSDictionary\NSDictionary_
+amos://E5567EFD-D62D-4ECC-9141-7E1152A04403
```



	name	change_id
-2A03-9B10-CBC4D9F13221	Seaslave	281474976710914
8-41D4-B204-A4153D3D4AE8	iCloud	0
0-A131-6D58-DB03D1021C79	aquanaut	0
2-438E-D15B-27525FED6D13	Seagypsy	0
9-8743-85D3-418AA6DD84E1	Seagypsy	0
1-787F-655E-970F9D65DA5D	jdp	0
3-0BDD-C073-B4FBEA8CE193	Seaslave	0
0-84E0-7F66-0497454653D6	jdp	2251799813685506
D-6C0C-AF07-829427FB26CE	aquanautold	2533274790396282
2-2C0E-D8F4-D13AC456311B	Seaslave	2814749767106818
4-12FE-06BA-D32343CD48AC	unknown4c8d79e54180	3096224743817474
D-640A-1E2A-564377FA352A	aquanaut	3377699720528371
C-B4B0-E06A-9A04AB3D8EEE	Seagypsy	0
4-45AA-AB3D-39AA29463E59	aquanaut	3940649673949442
8-EBC3-9A84-36839B3339A3	aquanaut	4222124650660675
3-468F-8E73-49600B522D94	Seagypsy	4503599627370754

GOT DATA?

(ANDROID)

LOC DATA (ANDROID)

2.3.4 GINGERBREAD

Location	Description
/data/data/<app name>	Application data
/data/data/com.android.providers.userdictionary	User dictionary, aka keyboard cache
/data/data/com.android.email	Email data – creds, messages, etc
/data/data/com.osp.app.signin	oAuth tokens, certs
/data/log	Error dumps
/data/misc/vpn	VPN profiles
/data/misc	Memory dumps
/data/system/sync	Sync accounts, sync targets (authorities)
/data/system/accounts.db	Account credentials, auth tokens, etc. (similar to KeyChain)
/data/wifi	Configured wifi networks – UID, PSK, etc
/dbdata/system/registered_services/packages.xml	Delegated permissions across device
/dbdata/databases/<app name>	Application database storage and preferences files
/dbdata/databases/com.android.providers.contacts	Accounts, contacts, calls
/dbdata/databases/com.android.providers.settings	Device settings
/dbdata/databases/com.android.providers.telephony	Mmssms details – sender/receiver, message, timestamp
/dbdata/databases/com.android.vending	Market downloads (account), carrier billing info
/dbdata/databases/com.google.android.gm	Gmail accounts, gmail data
/dbdata/databases/com.google.android.gsf	Google services settings, email disclosure
/dbdata/databases/com.sec.android.app.memo	Database of ‘memo’ entries
/dbdata/databases/com.sec.android.app.sns	Account information for social networking
/dbdata/databases/com.sec.android.provider.logsprovider	Log db
/dbdata/databases/com.sec.android.providers.drm	DRM details
/mnt/sdcard/data/browser	Browser cache tables and databases
/mnt/sdcard/data/crash	Crash logs
/mnt/sdcard/DCIM	Photos
/mnt/sdcard/Voodoo	Logs

LOC DATA (ANDROID)

4.0.4 ICE CREAM SANDWICH

Location	Description
/data/app/<appname>	user-installed APKs
/data/app-private/	user-installed apps with private storage
/data/misc	keychain, keystore, wifi, vpn - **Wifi creds still in the clear!**
/data/system	package permissions, entropy.dat?
/data/log	Error dumps
/data/misc/vpn	VPN profiles
/data/misc	Memory dumps
/data/misc/wifi	Configured wifi networks – SSID, UID, PSK, etc
/data/system/sync	Sync accounts, sync targets (authorities)
/data/system/accounts.db	Account creds, auth tokens, etc. - **Creds still in the clear!**
/data/system/packages.xml	Delegated permissions across apps
/datadata/<app name>	Applications and data (user and native)
/datadata/com.android.providers.userdictionary	User dictionary, aka keyboard cache
/datadata/com.android.email	Email data – creds, messages, etc
/datadata/com.google.android.gm	Gmail accounts, gmail data
/datadata/com.android.providers.contacts	Accounts, contacts, calls
/datadata/com.android.providers.settings	Device settings
/datadata/com.android.providers.telephony	Mmssms details – sender/receiver, message, timestamp
/datadata/com.android.vending	Market downloads (account), carrier billing info
/datadata/com.google.android.gsf	Google services settings, email disclosure
/datadata/com.sec.android.providers.drm	DRM details
/datadata/com.android.browser	cache, autofill, geo loc
/mnt/sdcard/DCIM	camera photos

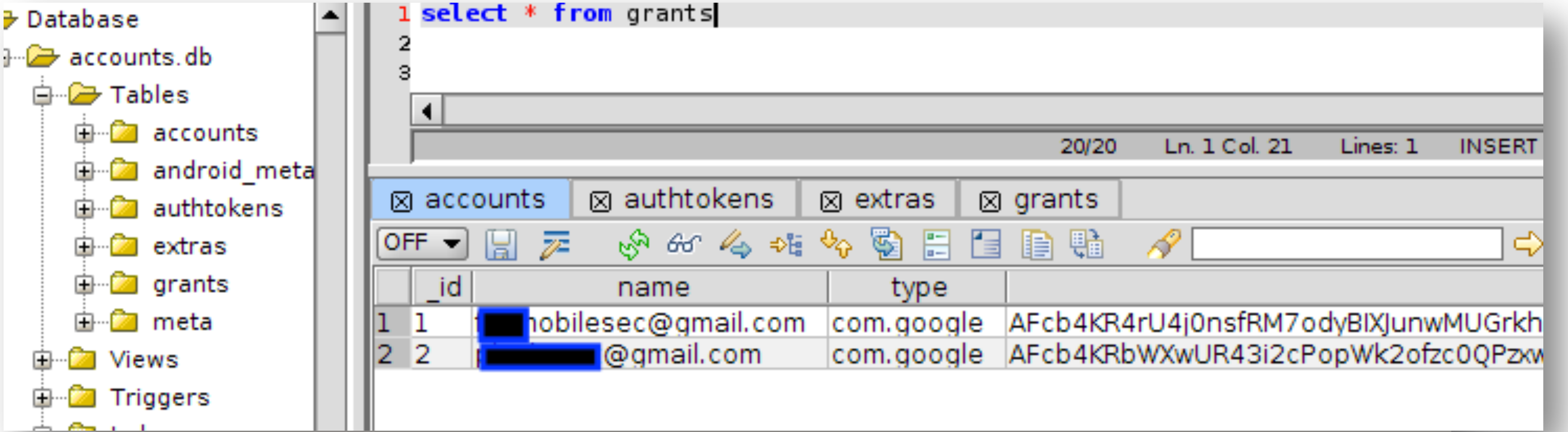
LOC DATA (ANDROID)

4.2.2 JELLY BEAN

Location	Description
/data/app/<appname>	user-installed APKs
/data/app-private/	user-installed apps with private storage
/data/misc	keychain, keystore, wifi, vpn - **Wifi creds still in the clear!**
/data/system	package permissions, entropy.dat?
/data/log	Error dumps
/data/misc/vpn	VPN profiles
/data/misc	Memory dumps
/data/misc/wifi	Configured wifi networks – SSID, UID, PSK, etc
/data/system/sync	Sync accounts, sync targets (authorities)
/data/system/accounts.db	Account creds, auth tokens, etc. - **Creds still in the clear!**
/data/system/packages.xml	Delegated permissions across apps
/datadata/<app name>	Applications and data (user and native)
/datadata/com.android.providers.userdictionary	User dictionary, aka keyboard cache
/datadata/com.android.email	Email data – creds, messages, etc
/datadata/com.google.android.gm	Gmail accounts, gmail data
/datadata/com.android.providers.contacts	Accounts, contacts, calls
/datadata/com.android.providers.settings	Device settings
/datadata/com.android.providers.telephony	Mmssms details – sender/receiver, message, timestamp
/datadata/com.android.vending	Market downloads (account), carrier billing info
/datadata/com.google.android.gsf	Google services settings, email disclosure
/datadata/com.sec.android.providers.drm	DRM details
/datadata/com.android.browser	cache, autofill, geo loc
/mnt/sdcard/DCIM	camera photos

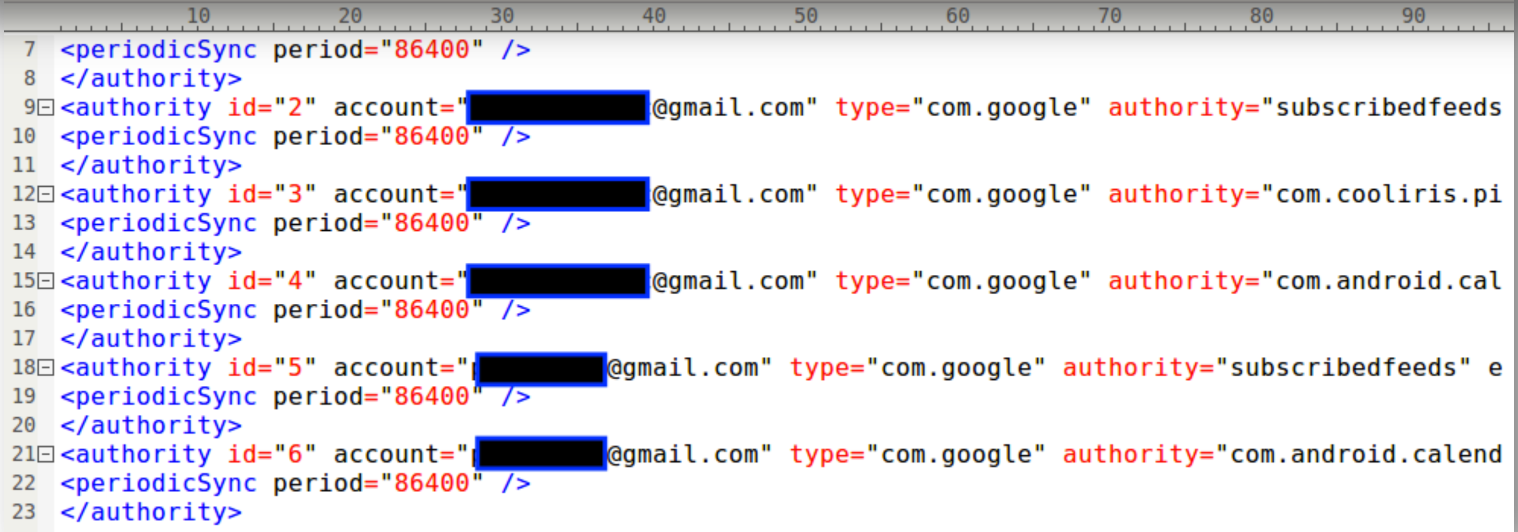
ANDROID FINDINGS!

ACCOUNTS



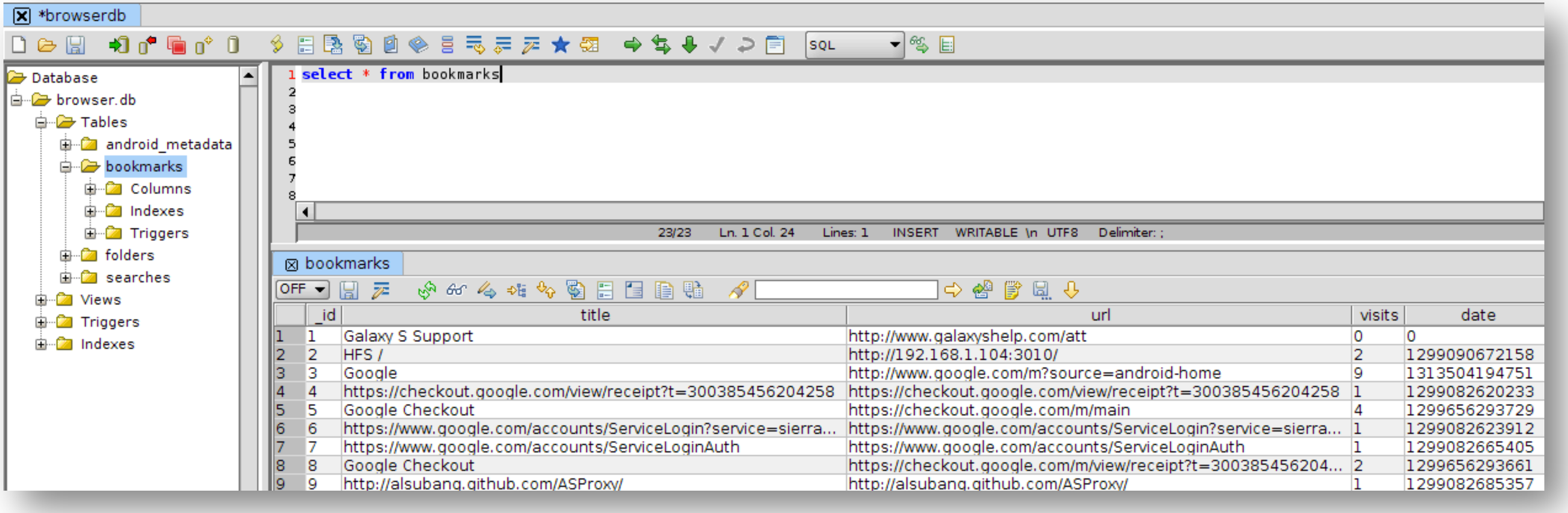
```
select * from grants
```

	_id	name	type	
1	1	[redacted]obilesec@gmail.com	com.google	AFcb4KR4rU4j0nsfRM7odyBIXJunwMUGrkh
2	2	[redacted]@gmail.com	com.google	AFcb4KRbWXwUR43i2cPopWk2ofzc0QPzxw



```
<periodicSync period="86400" />
</authority>
<authority id="2" account="[redacted]@gmail.com" type="com.google" authority="subscribedfeeds
<periodicSync period="86400" />
</authority>
<authority id="3" account="[redacted]@gmail.com" type="com.google" authority="com.cooliris.pi
<periodicSync period="86400" />
</authority>
<authority id="4" account="[redacted]@gmail.com" type="com.google" authority="com.android.cal
<periodicSync period="86400" />
</authority>
<authority id="5" account="[redacted]@gmail.com" type="com.google" authority="subscribedfeeds" e
<periodicSync period="86400" />
</authority>
<authority id="6" account="[redacted]@gmail.com" type="com.google" authority="com.android.calend
<periodicSync period="86400" />
</authority>
```

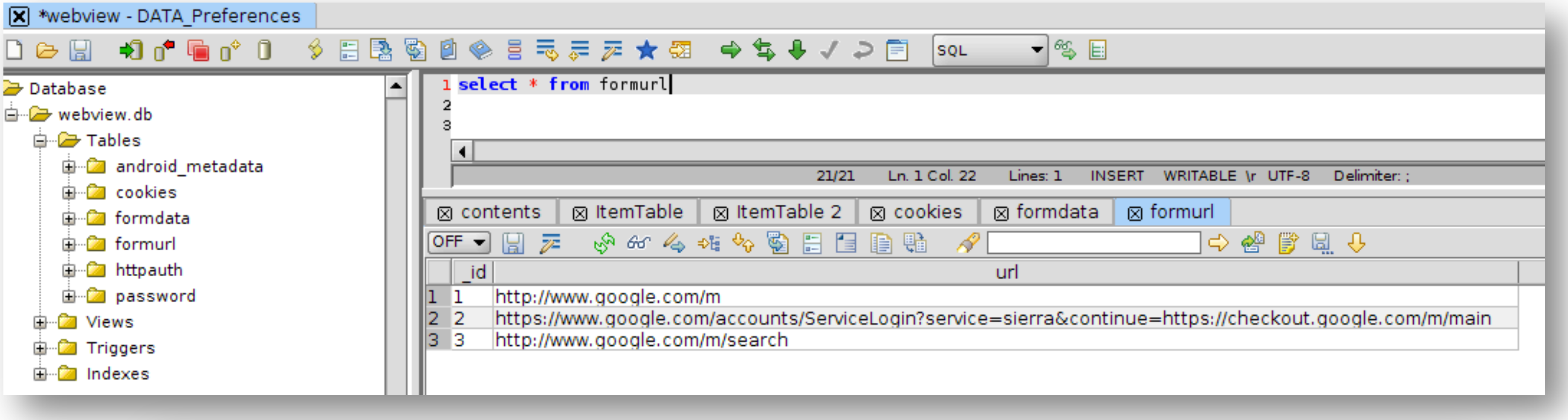
BOOKMARKS



```
select * from bookmarks
```

	_id	title	url	visits	date
1	1	Galaxy S Support	http://www.galaxyshelp.com/att	0	0
2	2	HFS /	http://192.168.1.104:3010/	2	1299090672158
3	3	Google	http://www.google.com/m?source=android-home	9	1313504194751
4	4	https://checkout.google.com/view/receipt?t=300385456204258	https://checkout.google.com/view/receipt?t=300385456204258	1	1299082620233
5	5	Google Checkout	https://checkout.google.com/m/main	4	1299656293729
6	6	https://www.google.com/accounts/ServiceLogin?service=sierra...	https://www.google.com/accounts/ServiceLogin?service=sierra...	1	1299082623912
7	7	https://www.google.com/accounts/ServiceLoginAuth	https://www.google.com/accounts/ServiceLoginAuth	1	1299082665405
8	8	Google Checkout	https://checkout.google.com/m/view/receipt?t=300385456204...	2	1299656293661
9	9	http://alsubang.github.com/ASProxy/	http://alsubang.github.com/ASProxy/	1	1299082685357

BROWSER DATA



☒ *webview - DATA_Preferences

Database
- webview.db
  - Tables
    - android_metadata
    - cookies
    - formdata
    - formurl
    - httpauth
    - password
  - Views
  - Triggers
  - Indexes

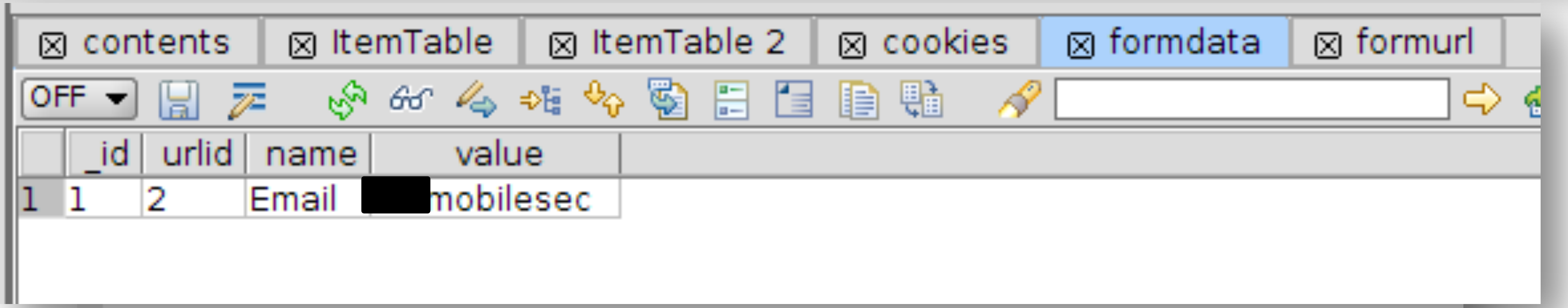
```
select * from formurl
```

21/21 Ln. 1 Col. 22 Lines: 1 INSERT WRITABLE \r UTF-8 Delimiter: ;

☒ contents ☒ ItemTable ☒ ItemTable 2 ☒ cookies ☒ formdata ☒ formurl

OFF

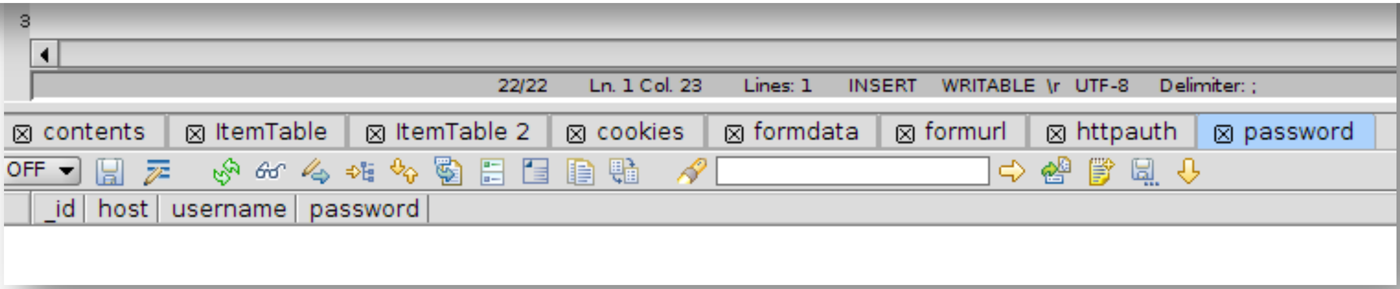
	_id	url
1	1	http://www.google.com/m
2	2	https://www.google.com/accounts/ServiceLogin?service=sierra&continue=https://checkout.google.com/m/main
3	3	http://www.google.com/m/search



☒ contents ☒ ItemTable ☒ ItemTable 2 ☒ cookies ☒ formdata ☒ formurl

OFF

	_id	urlid	name	value
1	1	2	Email	[redacted]mobilesec



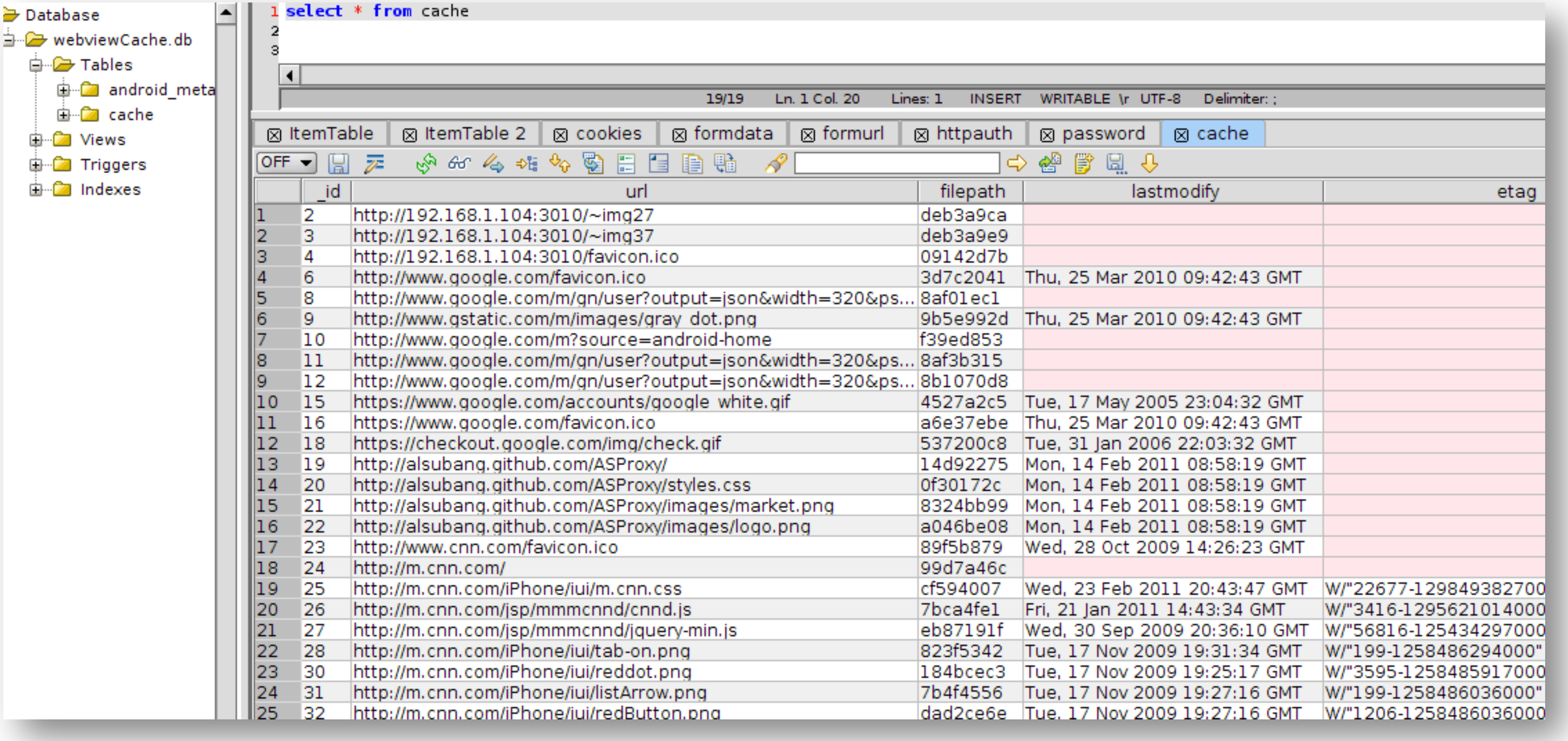
22/22 Ln. 1 Col. 23 Lines: 1 INSERT WRITABLE \r UTF-8 Delimiter: ;

☒ contents ☒ ItemTable ☒ ItemTable 2 ☒ cookies ☒ formdata ☒ formurl ☒ httpauth ☒ password

OFF

	_id	host	username	password

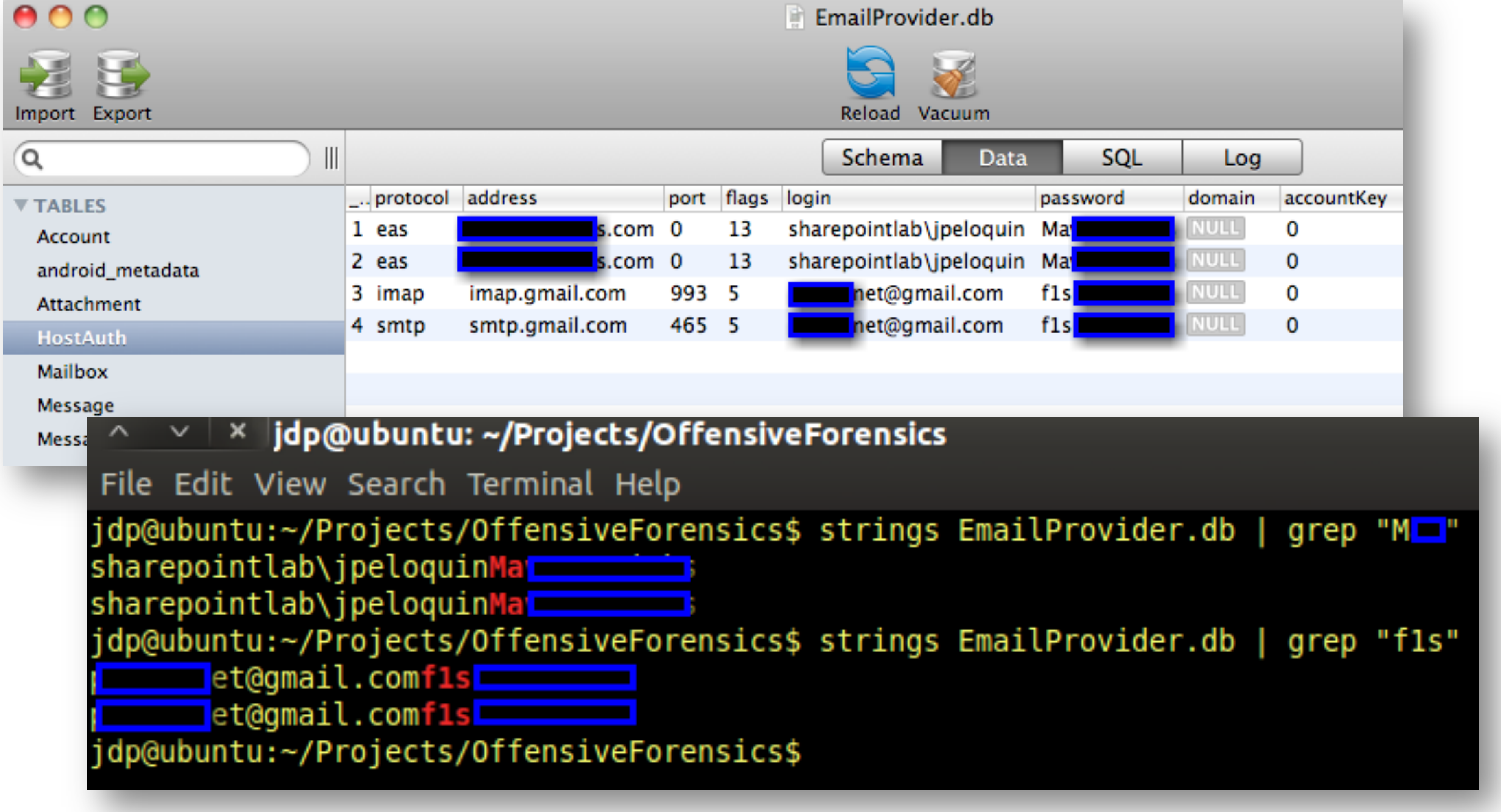
CACHE



```
1 select * from cache
2
3
```

	_id	url	filepath	lastmodify	etag
1	2	http://192.168.1.104:3010/~img27	deb3a9ca		
2	3	http://192.168.1.104:3010/~img37	deb3a9e9		
3	4	http://192.168.1.104:3010/favicon.ico	09142d7b		
4	6	http://www.google.com/favicon.ico	3d7c2041	Thu, 25 Mar 2010 09:42:43 GMT	
5	8	http://www.google.com/m/gn/user?output=json&width=320&ps...	8af01ec1		
6	9	http://www.gstatic.com/m/images/gray_dot.png	9b5e992d	Thu, 25 Mar 2010 09:42:43 GMT	
7	10	http://www.google.com/m?source=android-home	f39ed853		
8	11	http://www.google.com/m/gn/user?output=json&width=320&ps...	8af3b315		
9	12	http://www.google.com/m/gn/user?output=json&width=320&ps...	8b1070d8		
10	15	https://www.google.com/accounts/google_white.gif	4527a2c5	Tue, 17 May 2005 23:04:32 GMT	
11	16	https://www.google.com/favicon.ico	a6e37ebe	Thu, 25 Mar 2010 09:42:43 GMT	
12	18	https://checkout.google.com/img/check.gif	537200c8	Tue, 31 Jan 2006 22:03:32 GMT	
13	19	http://alsubang.github.com/ASProxy/	14d92275	Mon, 14 Feb 2011 08:58:19 GMT	
14	20	http://alsubang.github.com/ASProxy/styles.css	0f30172c	Mon, 14 Feb 2011 08:58:19 GMT	
15	21	http://alsubang.github.com/ASProxy/images/market.png	8324bb99	Mon, 14 Feb 2011 08:58:19 GMT	
16	22	http://alsubang.github.com/ASProxy/images/logo.png	a046be08	Mon, 14 Feb 2011 08:58:19 GMT	
17	23	http://www.cnn.com/favicon.ico	89f5b879	Wed, 28 Oct 2009 14:26:23 GMT	
18	24	http://m.cnn.com/	99d7a46c		
19	25	http://m.cnn.com/iPhone/iui/m.cnn.css	cf594007	Wed, 23 Feb 2011 20:43:47 GMT	W/"22677-129849382700
20	26	http://m.cnn.com/jsp/mmmcnnd/cnnd.js	7bca4fe1	Fri, 21 Jan 2011 14:43:34 GMT	W/"3416-129562101400C
21	27	http://m.cnn.com/jsp/mmmcnnd/jquery-min.js	eb87191f	Wed, 30 Sep 2009 20:36:10 GMT	W/"56816-125434297000
22	28	http://m.cnn.com/iPhone/iui/tab-on.png	823f5342	Tue, 17 Nov 2009 19:31:34 GMT	W/"199-1258486294000"
23	30	http://m.cnn.com/iPhone/iui/reddot.png	184bcec3	Tue, 17 Nov 2009 19:25:17 GMT	W/"3595-125848591700C
24	31	http://m.cnn.com/iPhone/iui/listArrow.png	7b4f4556	Tue, 17 Nov 2009 19:27:16 GMT	W/"199-1258486036000"
25	32	http://m.cnn.com/iPhone/iui/redButton.png	dad2ce6e	Tue, 17 Nov 2009 19:27:16 GMT	W/"1206-125848603600C

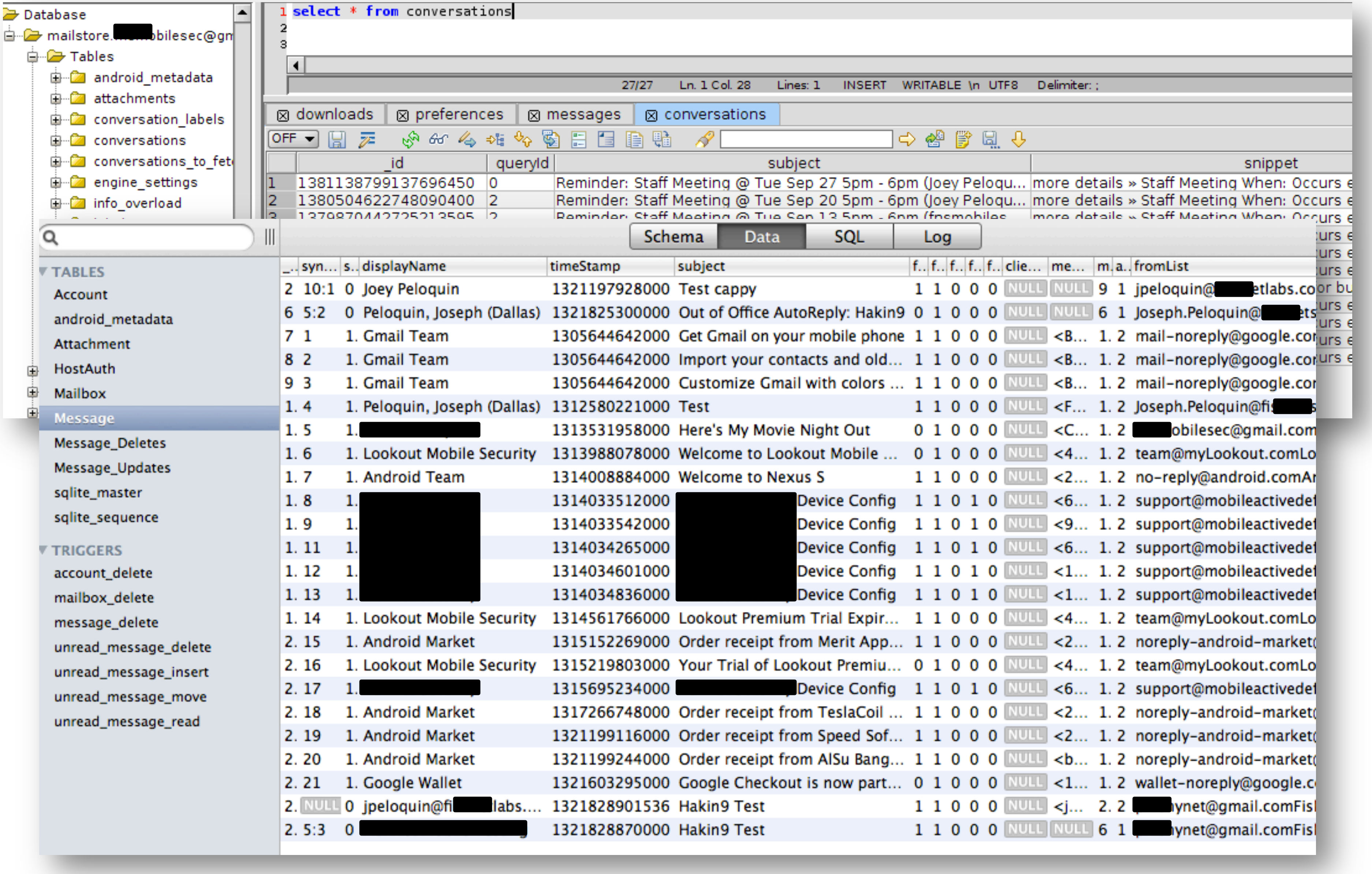
MAIL CREDS



_..	protocol	address	port	flags	login	password	domain	accountKey
1	eas	[redacted]s.com	0	13	sharepointlab\jpeloquin	Ma[redacted]	NULL	0
2	eas	[redacted]s.com	0	13	sharepointlab\jpeloquin	Ma[redacted]	NULL	0
3	imap	imap.gmail.com	993	5	[redacted]net@gmail.com	f1s[redacted]	NULL	0
4	smtp	smtp.gmail.com	465	5	[redacted]net@gmail.com	f1s[redacted]	NULL	0

```
jdp@ubuntu:~/Projects/OffensiveForensics$ strings EmailProvider.db | grep "M[redacted]"
sharepointlab\jpeloquinMa[redacted]
sharepointlab\jpeloquinMa[redacted]
jdp@ubuntu:~/Projects/OffensiveForensics$ strings EmailProvider.db | grep "f1s"
[redacted]et@gmail.comf1s[redacted]
[redacted]et@gmail.comf1s[redacted]
jdp@ubuntu:~/Projects/OffensiveForensics$
```

MAIL



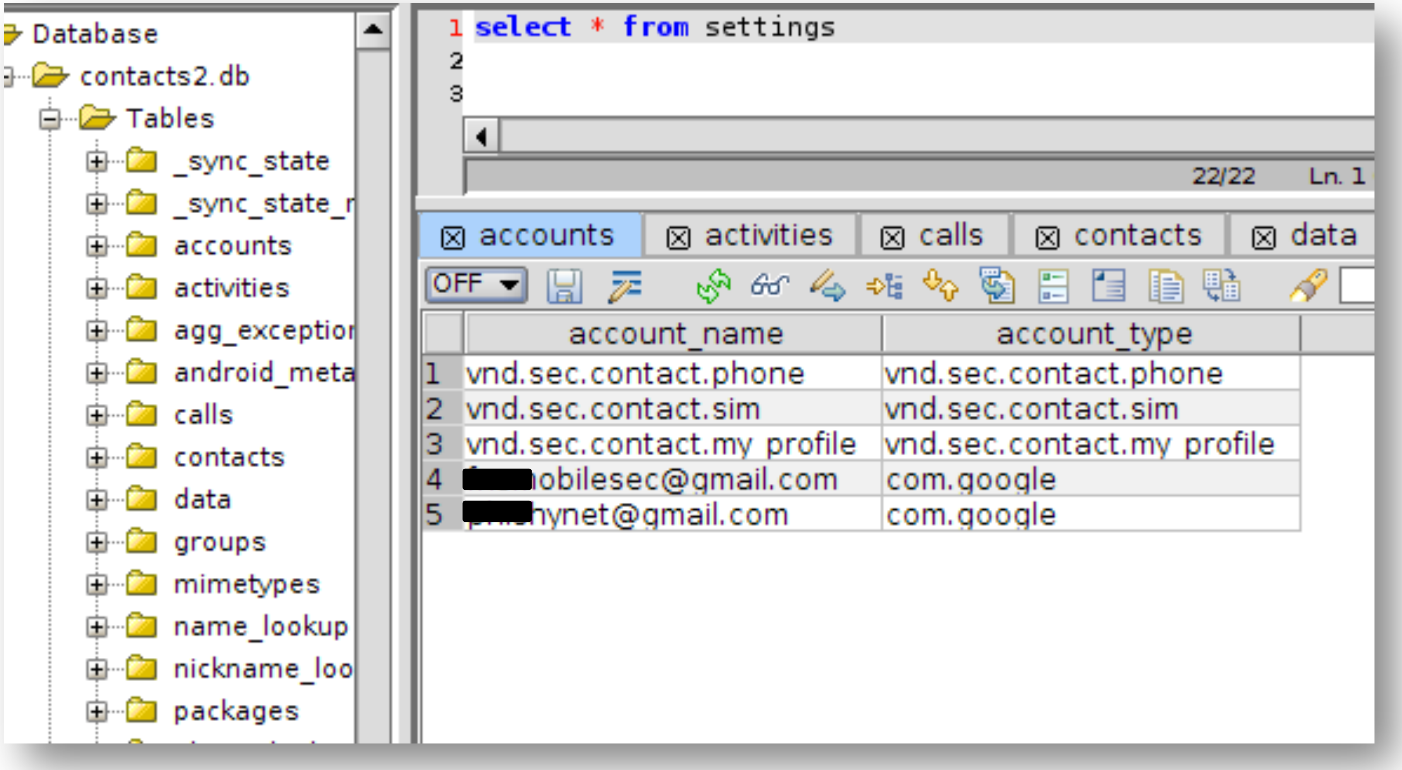
```
1 select * from conversations
2
3
```

```
27/27    Ln. 1 Col. 28    Lines: 1    INSERT    WRITABLE \n  UTF8    Delimiter: ;
```

	_id	queryId	subject	snippet
1	1381138799137696450	0	Reminder: Staff Meeting @ Tue Sep 27 5pm - 6pm (Joey Pelequ…	more details » Staff Meeting When: Occurs e
2	1380504622748090400	2	Reminder: Staff Meeting @ Tue Sep 20 5pm - 6pm (Joey Pelequ…	more details » Staff Meeting When: Occurs e
3	1379870442725213595	2	Reminder: Staff Meeting @ Tue Sep 13 5pm - 6pm (fpsmobiles	more details » Staff Meeting When: Occurs e

_..	syn…	s..	displayName	timeStamp	subject	f..	f..	f..	f..	f..	clie…	me…	m.	a..	fromList
2	10:1	0	Joey Peloquin	1321197928000	Test cappy	1	1	0	0	0	NULL	NULL	9	1	jpeloquin@[redacted]etlabs.co
6	5:2	0	Peloquin, Joseph (Dallas)	1321825300000	Out of Office AutoReply: Hakin9	0	1	0	0	0	NULL	NULL	6	1	Joseph.Peloquin@[redacted]ets
7	1	1.	Gmail Team	1305644642000	Get Gmail on your mobile phone	1	1	0	0	0	NULL	<B…	1.	2	mail-noreply@google.cor
8	2	1.	Gmail Team	1305644642000	Import your contacts and old…	1	1	0	0	0	NULL	<B…	1.	2	mail-noreply@google.cor
9	3	1.	Gmail Team	1305644642000	Customize Gmail with colors …	1	1	0	0	0	NULL	<B…	1.	2	mail-noreply@google.cor
1.	4	1.	Peloquin, Joseph (Dallas)	1312580221000	Test	1	1	0	0	0	NULL	<F…	1.	2	Joseph.Peloquin@fi[redacted]s
1.	5	1.	[redacted]	1313531958000	Here's My Movie Night Out	0	1	0	0	0	NULL	<C…	1.	2	[redacted]obilesec@gmail.com
1.	6	1.	Lookout Mobile Security	1313988078000	Welcome to Lookout Mobile …	0	1	0	0	0	NULL	<4…	1.	2	team@myLookout.comLo
1.	7	1.	Android Team	1314008884000	Welcome to Nexus S	1	1	0	0	0	NULL	<2…	1.	2	no-reply@android.comAr
1.	8	1.	[redacted]	1314033512000	[redacted]Device Config	1	1	0	1	0	NULL	<6…	1.	2	support@mobileactivedef
1.	9	1.	[redacted]	1314033542000	[redacted]Device Config	1	1	0	1	0	NULL	<9…	1.	2	support@mobileactivedef
1.	11	1.	[redacted]	1314034265000	[redacted]Device Config	1	1	0	1	0	NULL	<6…	1.	2	support@mobileactivedef
1.	12	1.	[redacted]	1314034601000	[redacted]Device Config	1	1	0	1	0	NULL	<1…	1.	2	support@mobileactivedef
1.	13	1.	[redacted]	1314034836000	[redacted]Device Config	1	1	0	1	0	NULL	<1…	1.	2	support@mobileactivedef
1.	14	1.	Lookout Mobile Security	1314561766000	Lookout Premium Trial Expir…	1	1	0	0	0	NULL	<4…	1.	2	team@myLookout.comLo
2.	15	1.	Android Market	1315152269000	Order receipt from Merit App…	1	1	0	0	0	NULL	<2…	1.	2	noreply-android-market(
2.	16	1.	Lookout Mobile Security	1315219803000	Your Trial of Lookout Premiu…	0	1	0	0	0	NULL	<4…	1.	2	team@myLookout.comLo
2.	17	1.	[redacted]	1315695234000	[redacted]Device Config	1	1	0	1	0	NULL	<6…	1.	2	support@mobileactivedef
2.	18	1.	Android Market	1317266748000	Order receipt from TeslaCoil …	1	1	0	0	0	NULL	<2…	1.	2	noreply-android-market(
2.	19	1.	Android Market	1321199116000	Order receipt from Speed Sof…	1	1	0	0	0	NULL	<2…	1.	2	noreply-android-market(
2.	20	1.	Android Market	1321199244000	Order receipt from AlSu Bang…	1	1	0	0	0	NULL	<b…	1.	2	noreply-android-market(
2.	21	1.	Google Wallet	1321603295000	Google Checkout is now part…	0	1	0	0	0	NULL	<1…	1.	2	wallet-noreply@google.c
2.	NULL	0	jpeloquin@fi[redacted]labs.…	1321828901536	Hakin9 Test	1	1	0	0	0	NULL	<j…	2.	2	[redacted]ynet@gmail.comFis
2.	5:3	0	[redacted]	1321828870000	Hakin9 Test	1	1	0	0	0	NULL	NULL	6	1	[redacted]ynet@gmail.comFis

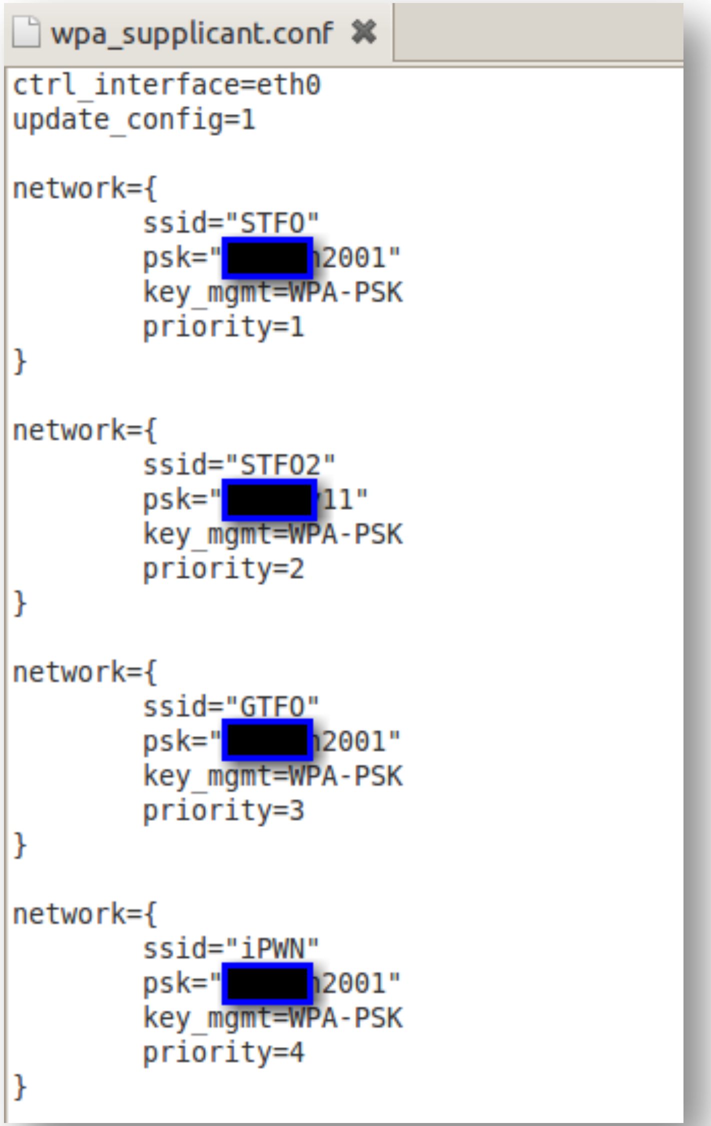
CONTACTS



```
select * from settings
```

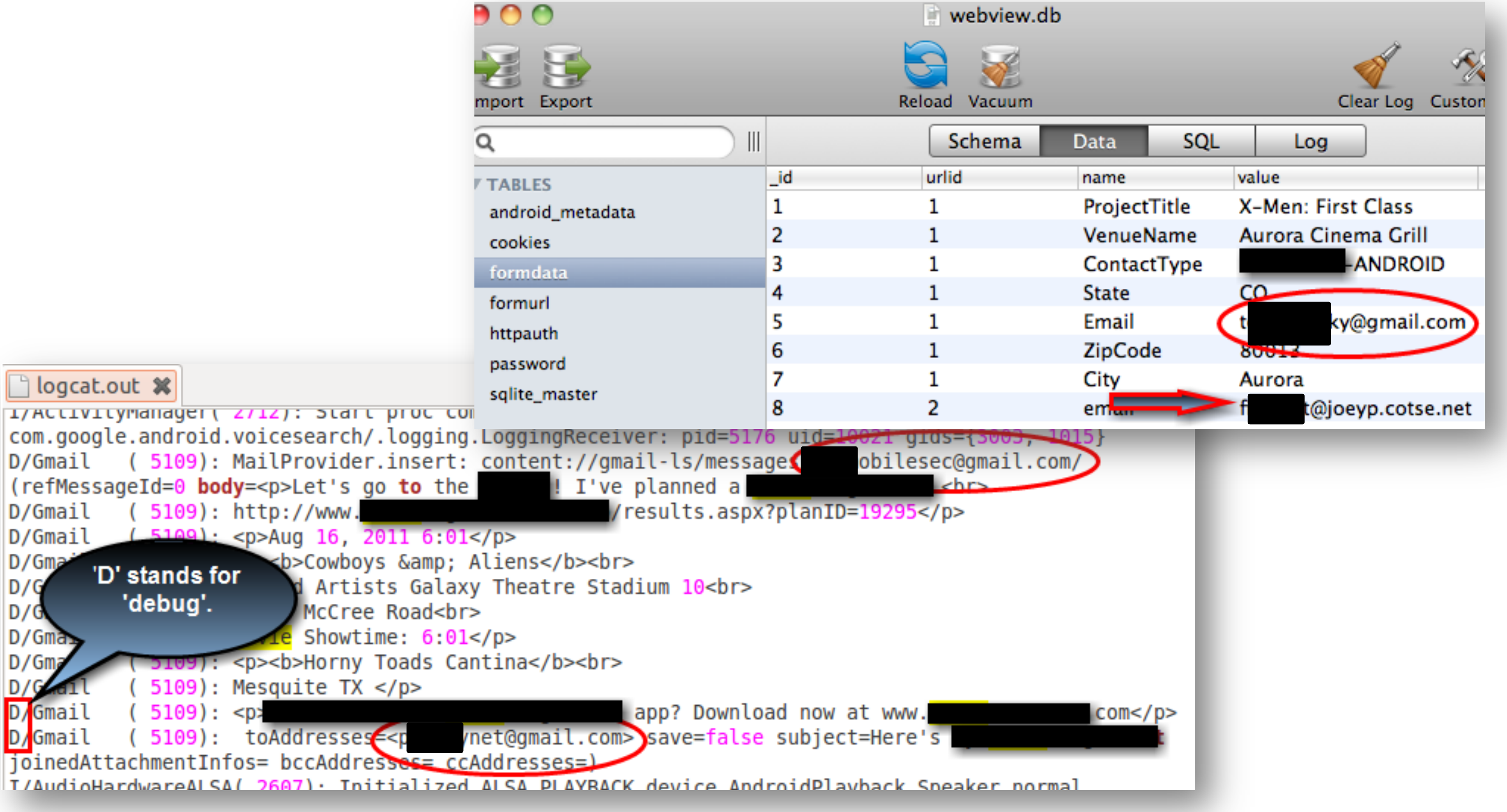
	account_name	account_type
1	vnd.sec.contact.phone	vnd.sec.contact.phone
2	vnd.sec.contact.sim	vnd.sec.contact.sim
3	vnd.sec.contact.my_profile	vnd.sec.contact.my_profile
4	[redacted]obilesec@gmail.com	com.google
5	[redacted]ynet@gmail.com	com.google

WIFI CONFIG



```
ctrl_interface=eth0
update_config=1

network={
        ssid="STFO"
        psk="[redacted]2001"
        key_mgmt=WPA-PSK
        priority=1
}

network={
        ssid="STFO2"
        psk="[redacted]11"
        key_mgmt=WPA-PSK
        priority=2
}

network={
        ssid="GTFO"
        psk="[redacted]2001"
        key_mgmt=WPA-PSK
        priority=3
}

network={
        ssid="iPWN"
        psk="[redacted]2001"
        key_mgmt=WPA-PSK
        priority=4
}
```

APPLICATIONS

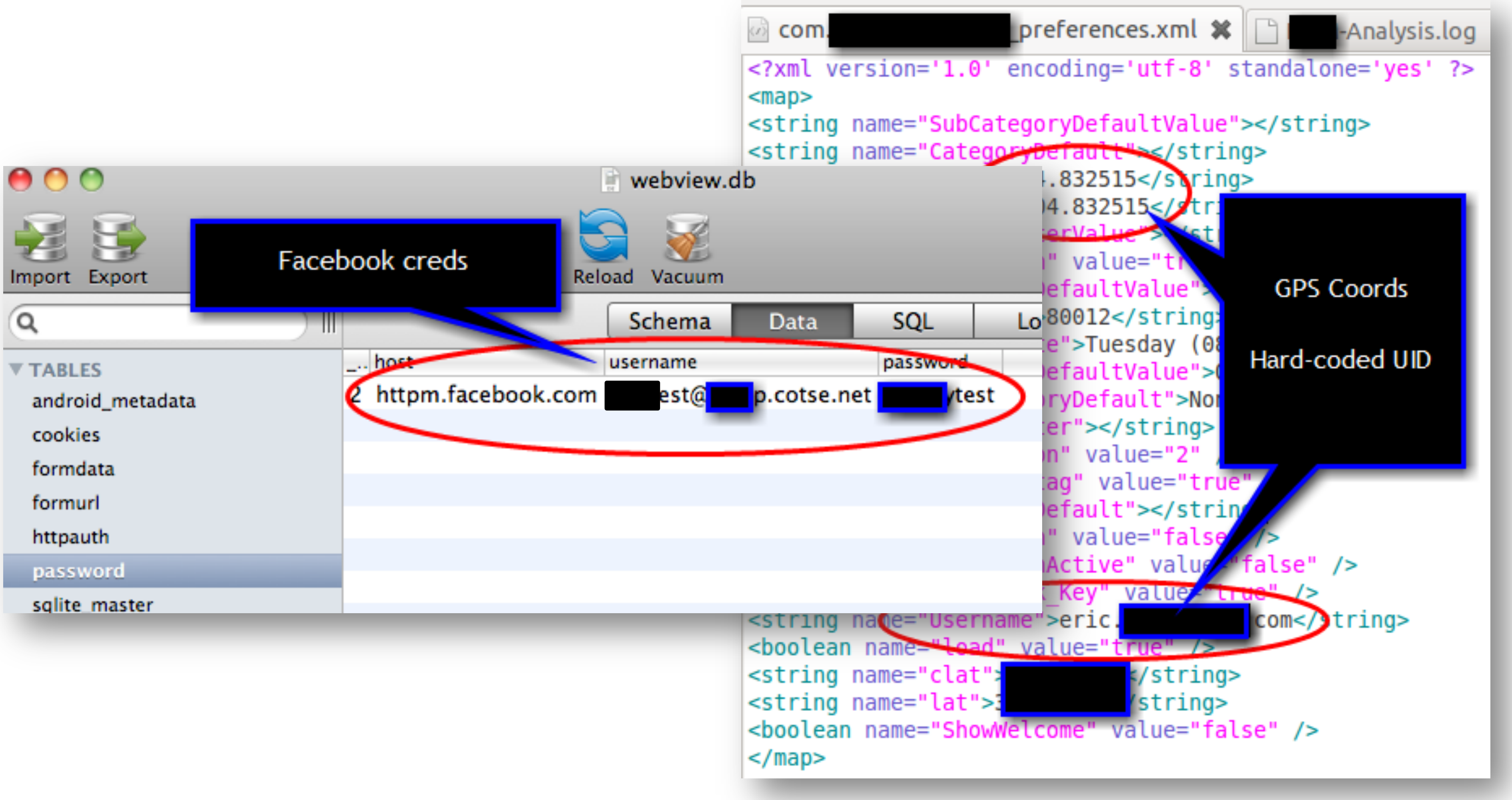


_id	urlid	name	value
1	1	ProjectTitle	X-Men: First Class
2	1	VenueName	Aurora Cinema Grill
3	1	ContactType	[redacted]-ANDROID
4	1	State	CO
5	1	Email	t[redacted]ky@gmail.com
6	1	ZipCode	[redacted]
7	1	City	Aurora
8	2	email	f[redacted]t@joeyp.cotse.net

```
I/ActivityManager( 2712): Start proc com
com.google.android.voicesearch/.logging.LoggingReceiver: pid=5176 uid=10021 gids={3003, 1015}
D/Gmail    ( 5109): MailProvider.insert: content://gmail-ls/messages[redacted]obilesec@gmail.com/
(refMessageId=0 body=<p>Let's go to the [redacted]! I've planned a [redacted] <br>
D/Gmail    ( 5109): http://www.[redacted]/results.aspx?planID=19295</p>
D/Gmail    ( 5109): <p>Aug 16, 2011 6:01</p>
D/Gma                <b>Cowboys &amp; Aliens</b><br>
D/G                 d Artists Galaxy Theatre Stadium 10<br>
D/G                  McCree Road<br>
D/Gma               vie Showtime: 6:01</p>
D/Gma      ( 5109): <p><b>Horny Toads Cantina</b><br>
D/Gmail    ( 5109): Mesquite TX </p>
D/Gmail    ( 5109): <p[redacted] app? Download now at www.[redacted]com</p>
D/Gmail    ( 5109):  toAddresses=<p[redacted]ynet@gmail.com> save=false subject=Here's [redacted]
joinedAttachmentInfos= bccAddresses= ccAddresses=)
I/AudioHardwareALSA( 2607): Initialized ALSA PLAYBACK device AndroidPlayback Speaker normal
```

'D' stands for 'debug'.

APPLICATIONS



_..	host	username	password
2	httpm.facebook.com	[redacted]est@[redacted]p.cotse.net	[redacted]ytest

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
<string name="SubCategoryDefaultValue"></string>
<string name="CategoryDefault"></string>
.832515</string>
4.832515</stri
erValue"></st
n" value="t
efaultValue"
80012</string
e">Tuesday (0
efaultValue">
ryDefault">No
er"></string>
n" value="2"
ag" value="true"
efault"></strin
" value="false" />
Active" value="false" />
_Key" value="true" />
<string name="Username">eric.[redacted]com</string>
<boolean name="load" value="true" />
<string name="clat">[redacted]</string>
<string name="lat">3[redacted]string>
<boolean name="ShowWelcome" value="false" />
</map>
```

Facebook creds

GPS Coords

Hard-coded UID

It's OKay
I'm Scared Too

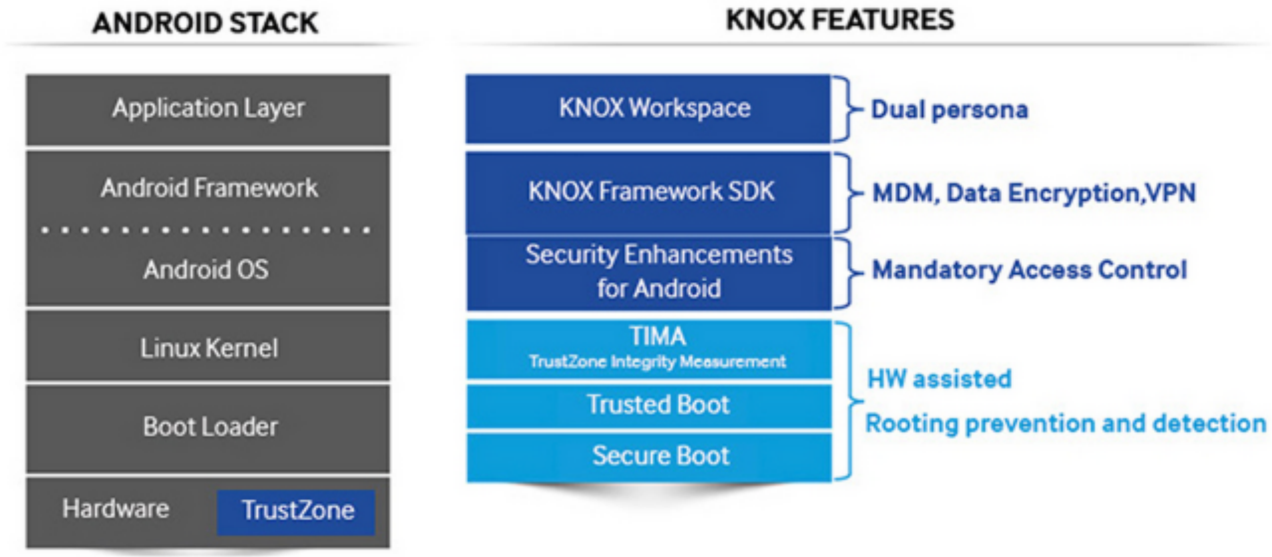
MITIGATION

- MOBILE SECURITY POLICY
- MOBILE SECURITY EDUCATION
- ~~MOBILE DEVICE MANAGEMENT~~
  - MADIM (APP + DEVICE + INFO)
- OFFENSIVE MOBILE FORENSICS
- SECURE MOBILE DEVELOPMENT

"In the popular culture, the availability of 10,000 applications for my smart phone is viewed as an unalloyed good. It is not — since each represents a potential vulnerability. But if we want to shift the popular culture, we need a broader flow of information to corporations and individuals to educate them on the threat. To do that we need to recalibrate what is truly secret."

– *Gen. Michael Hayden, ret.*

SAMSUNG KNOX



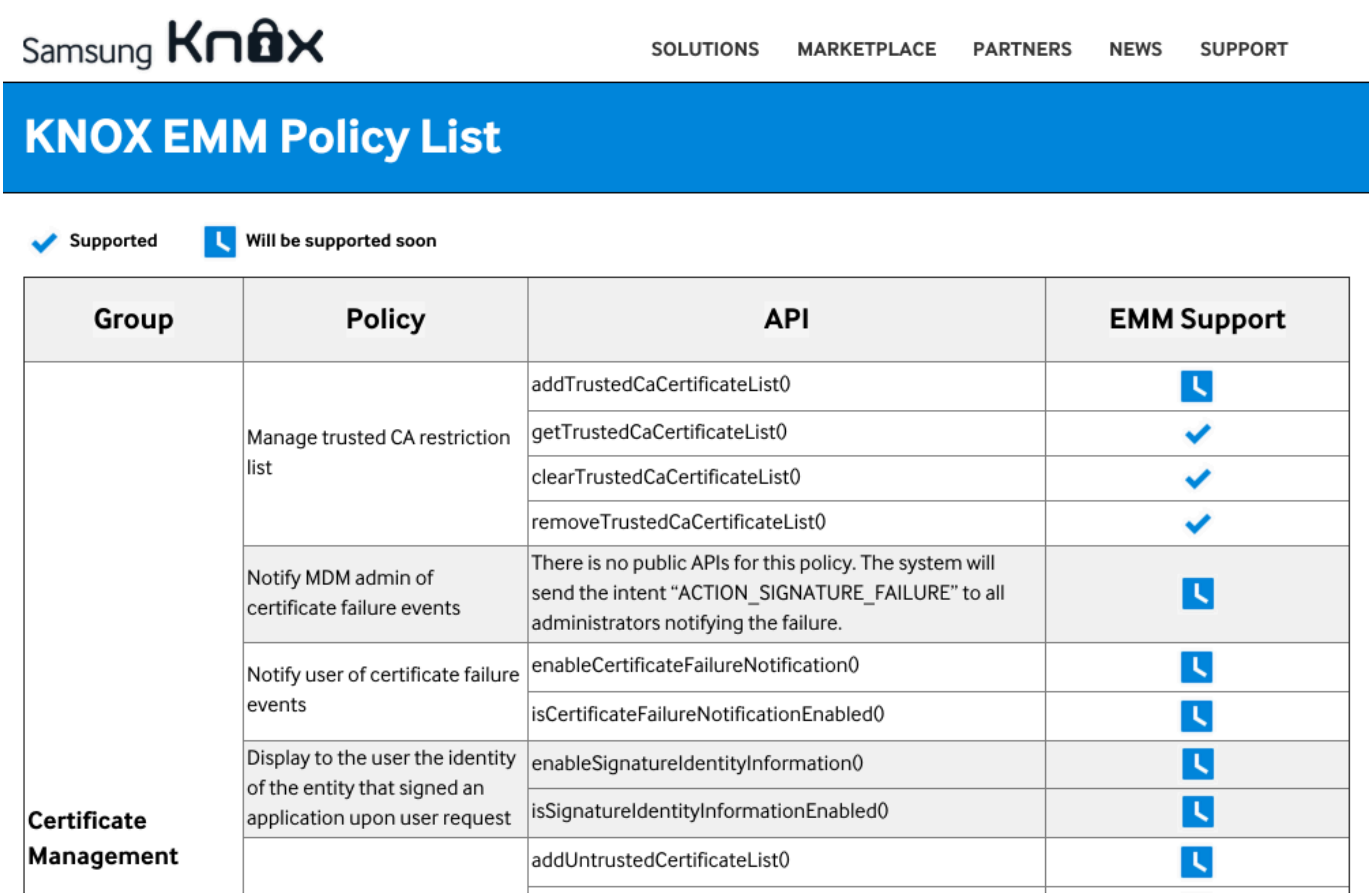
- SECURED BOOTLOADER
  - 0X0, 0X1
- REMOVE? DISABLE?
- KERNELS AND RECOVERIES
- CONTAINER; DUAL PERSONA SYSTEM

SAMSUNG KNOX

KNOX 2.0

- S5
- WORKSPACE
- EMM
- MARKETPLACE
- CUSTOMIZATION

SAMSUNG KNOX

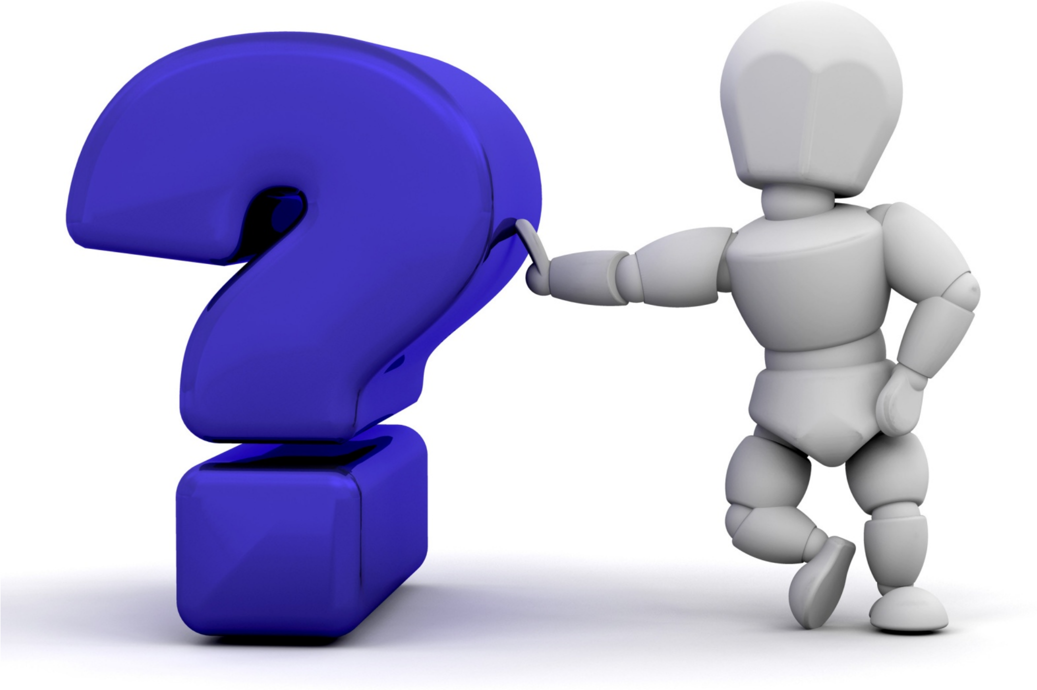


KNOX EMM Policy List

✓ Supported   🕓 Will be supported soon

Group	Policy	API	EMM Support
Certificate Management	Manage trusted CA restriction list	addTrustedCaCertificateList()	🕓
		getTrustedCaCertificateList()	✓
		clearTrustedCaCertificateList()	✓
		removeTrustedCaCertificateList()	✓
	Notify MDM admin of certificate failure events	There is no public APIs for this policy. The system will send the intent “ACTION_SIGNATURE_FAILURE” to all administrators notifying the failure.	🕓
	Notify user of certificate failure events	enableCertificateFailureNotification()	🕓
		isCertificateFailureNotificationEnabled()	🕓
	Display to the user the identity of the entity that signed an application upon user request	enableSignatureIdentityInformation()	🕓
		isSignatureIdentityInformationEnabled()	🕓
		addUntrustedCertificateList()	🕓

THANK YOU!



JOEY PELOQUIN

JOEY@GUIDEPOINTSECURITY.COM