Deep "geek" diving into the iPhone OS and Frameworks

Tim Burks

360iDev

March 3, 2009

Tips for digging deep

tim@neontology.com

Welcome, Silicon Valley iPhone Developers!

Location
Palo Alto, CA

Members
751 iPhone Developers

Meetup topics
Software Developers

Meetups
13 so far

Rating

Founded
March 7, 2008

We get together monthly to share projects, opportunities, and how-tos related to developing for the iPhone. Experienced developers, newcomers, and people with ideas are all welcome. We've enjoyed presentations from investors, entrepreneurs, and experts in all sorts of relevant topics from user interface design to programming. Each meeting usually contains a couple of fast-paced but deep talks and several demos. We don't do a lot of detailed programming instruction (there are lots of other resources for that), but instead focus on getting iPhone developers and entrepreneurs together with each other and with the resources they need to succeed. Got an iPhone project? Come join us!

Our next Meetup

iPhone Developers' Meetup

Mar 16
Mon 6:30 PM

Where?
This location is shown only to members

Who's coming?
98 Yes / **1 Maybe**
(31 spots left)

Want to attend?
Join us!

Meetup opens at 6:30, talks start at 7:00.

More details about this Meetup...

Silicon Valley iPhone Developer's Meetup

- 3rd Monday of the month
- TIPS group, Palo Alto
- Demos, technical, business talks
- meetup.com/sviphone

tim@neontology.com

MAGMA. Design Ahead of the Curve™

Worldwide Sites | Sales | MOLTEN Online Support | Contact Us | RSS | Search »

PRODUCTS AND SOLUTIONS | SUPPORT AND TRAINING | RESOURCES | PARTNERS | USERS GROUP | COMPANY

Webinar: Talus Vortex

The fastest throughput for multi-mode, multi-corner design closure.

» View now

Vortex Webinar

MUSIC

Earnings Call

QUICKLINKS

- MOLTEN Online Support »
- Global Training »
- Careers »
- Investor Relations »

NEWS

VIEW ALL »

Magma: Magma Beats Guidance for Third Quarter with Revenue of $30.7 Million

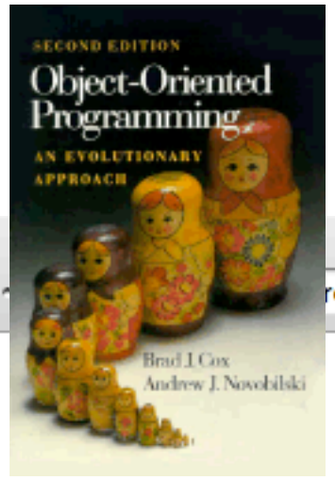
FEATURED PRODUCTS

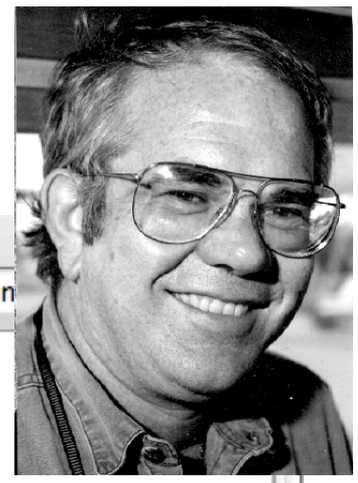
VIEW ALL »

Digital IC

Talus Vortex

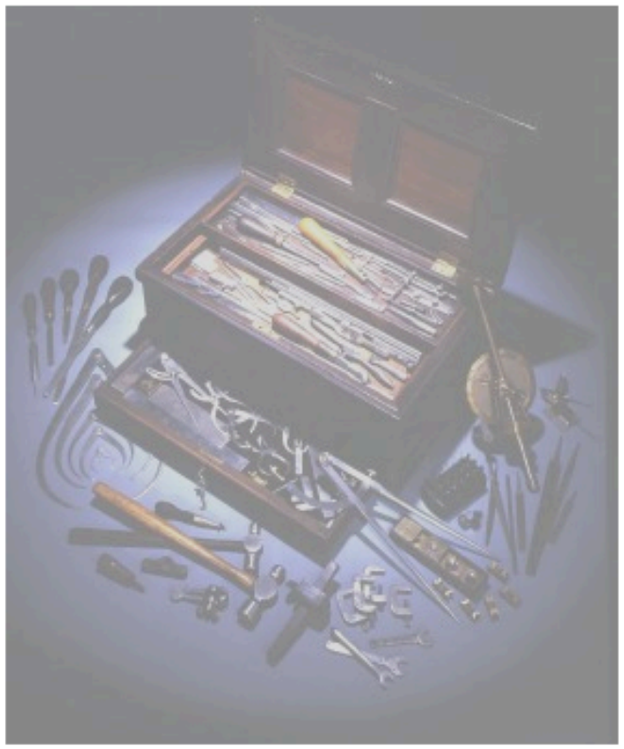
This physical design environment enables rapid development of netlist- and chip-level constraints





Planning the Software Industrial Revolution

http://www.virtualschool.edu/cox/pub/PSIR/



Planning the Software Industrial Revolution

by Brad J. Cox Ph.D

November 1990
IEEE Software magazine
Software Technologies of the 1990's.

Also see Technology Transition: A Historical Perspective by Allan Willey

The possibility of a software industrial revolution, in which programmers stop coding everything from scratch and begin assembling applications from well-stocked catalogs of reusable software components, is an enduring dream that continues to elude our grasp. Although object-oriented programming has brought the software industrial revolution a step closer, common-sense organizational principles like reusability and interchangeability are still the exception rather than the rule.

According to the historian, Thomas Kuhn, science does not progress continuously, by gradually extending an established paradigm. It proceeds as a series of revolutionary upheavals[KUHN]. The discovery of unreconcilable shortcomings in an established paradigm produces a crisis that may lead to a revolution in which the established paradigm is overthrown and replaced.

Addendum: May 2001

When I wrote this article I was only beginning to be aware of the far-reaching implications of a key difference between industrial and information age goods. Industrial age goods are made of atoms that

RubyCocoa Resources

http://www.rubycocoa.com/

RSS

rubycocoa

RubyCocoa Resources

beautiful applications, beautiful code

The Object-Oriented Scripting Language

Ruby

About this site

Do you want to write a Cocoa application with Ruby?

This web site will help you get started. [more]

An Intro

Develop beau

Writing

With RubyCo

Ruby Ro

Build a simpl

The Rub

Use RubyCoc

Rubifica

See more exa

Cocoa M

RubyObjC. A Ruby/Objective-C bridge.

http://www.rubyobjc.com/history

rubycocoa

RubyObjC. A Ruby/Objective-C bridge.

HOME | ABOUT RUBYOBJC | EXAMPLES | DOCUMENTATION | GUIDES | HISTORY | CONTACT

RubyObjC release history.

RubyObjC-0.4.0, June 10, 2007

- New **ObjC::Variable** class to wrap Objective-C instance variable descriptions.
- **ivars** and **ivar** methods for accessing Objective-C instance variables directly.
- Fixed Rake task to support application names that contain spaces.
- Improved Rake task that allows source code to be organized in directories named objc, ruby, and resources.
- Faster bridge crossings from Ruby to Objective-C.
- Improved handling of method calls with incorrect argument counts.
- RubyObjC screen saver example.
- Ruby plugins for Objective-C programs (screenshot below).

Install the gem.

```
% sudo gem install rubyobjc \
--source http://www.rubyobjc.com
```

Create an application.

```
% rubyapp myapp
```

Build it.

```
% cd myapp; rake
```

Run.

```
% rake run
```

My Yahoo!

http://my.yahoo.com/

Google

MY local

RubyObjC Console


Programming Nu
http://programming.nu/
RSS
rubycocoa
Programming Nu™
Website for the Nu programming language.
About Nu™
About Me
twitter.com/timburks
del.icio.us/timburks
blog.neontology.com
tootsweet software
OHLOH PROFILE
Community
Google Group:
Programming Nu
Macros
Friday, 02 Jan 2009
Thanks to Jeff Buck and Issac Trotts, we have some nice changes coming to Nu macros.
The changes are modeled on the description of macros in Paul Graham's On Lisp, so our new macro facility should feel familiar to experienced Lisp programmers.
Currently the changes are in my (Tim's) git repository, and they'll be included in the next release of Nu (0.4.0).
For more detail, see Jeff's excellent tutorial.

What's Nu?

Nu is an interpreted object-oriented language. Its syntax comes from Lisp, but Nu is semantically closer to Ruby than Lisp. Nu is implemented in Objective-C and is designed to take full advantange of the Objective-C runtime and the many mature class libraries written in Objective-C. Nu code can fully interoperate with code written in Objective-C; messages can be sent to and from objects with no concern for whether those messages are implemented in Objective-C or Nu.

timburks's nu at master - GitHub

git http://github.com/timburks/nu/tree/master RSS Google

github SOCIAL CODING

Search

Browse | Guides | Advanced

timburks

17

account | profile | log out

dashboard | gists

Source | Commits | Network (16) | Fork Queue | Downloads (0) | Wiki (1) | Graphs | Admin

master all branches all tags

timburks / nu edit pull request unwatch download 99 16

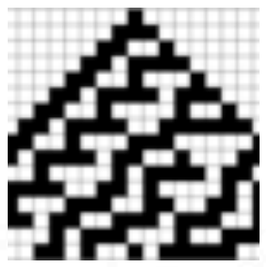
Description: The Nu programming language. edit

Homepage: http://programming.nu edit

Public Clone URL: git://github.com/timburks/nu.git

tim@neontology.com

Nu Who's Who



Jeff Buck (itfrombit)

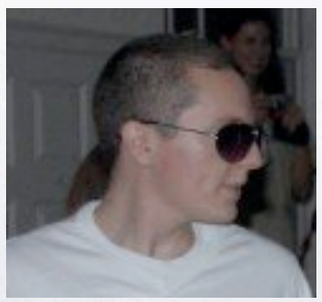
OpenGL, macros (with Issac Trotts)

Jason Sallis (jsallis)

TextMate bundle, nuke

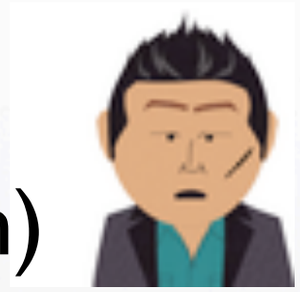
Patrick Thomson (importantshock)

Nu, YAML, applications



Grayson Hansard (grayson)

Markdown, nug (Nu->ObjC header file generator)

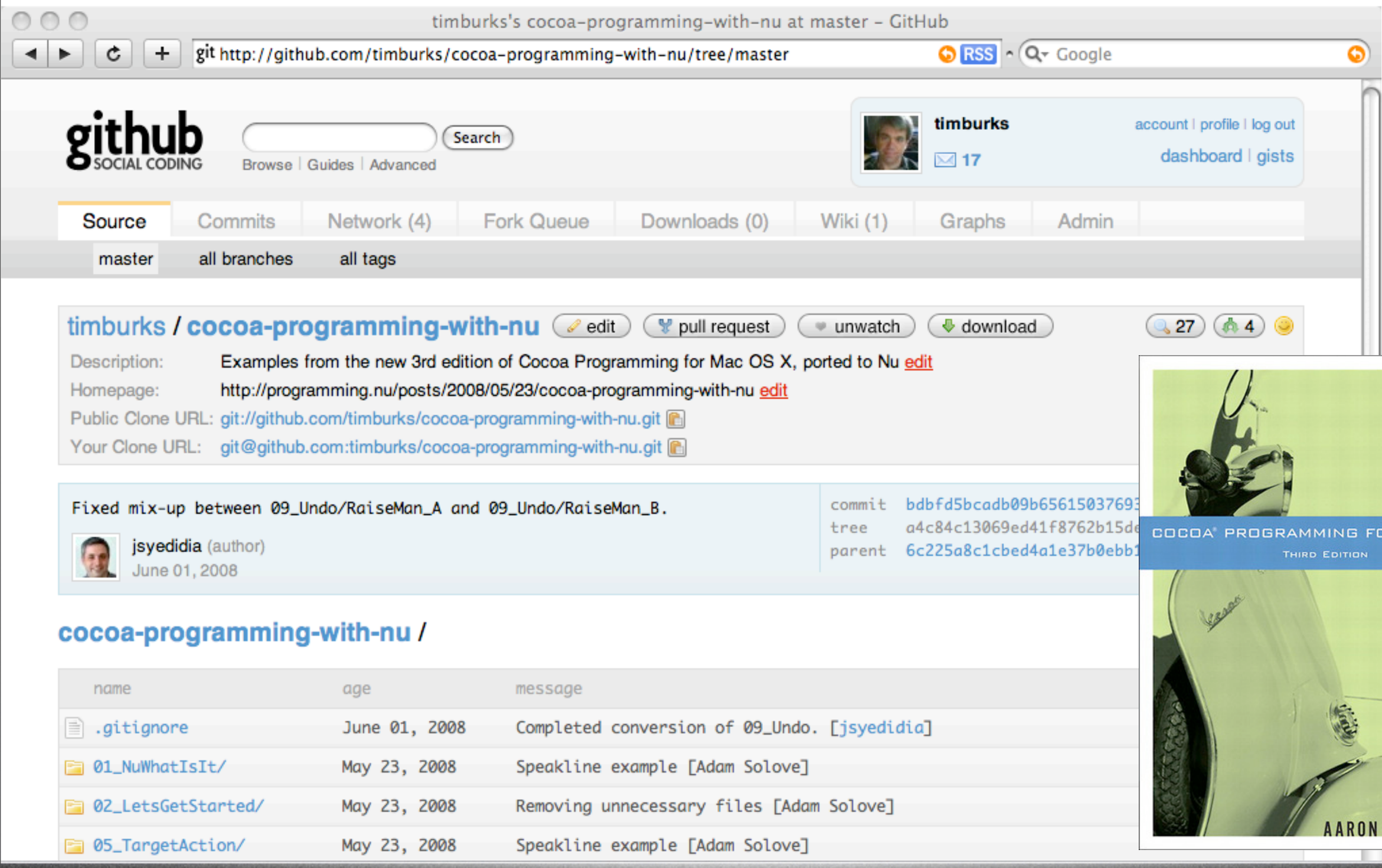


Dean Mao (deanmao)

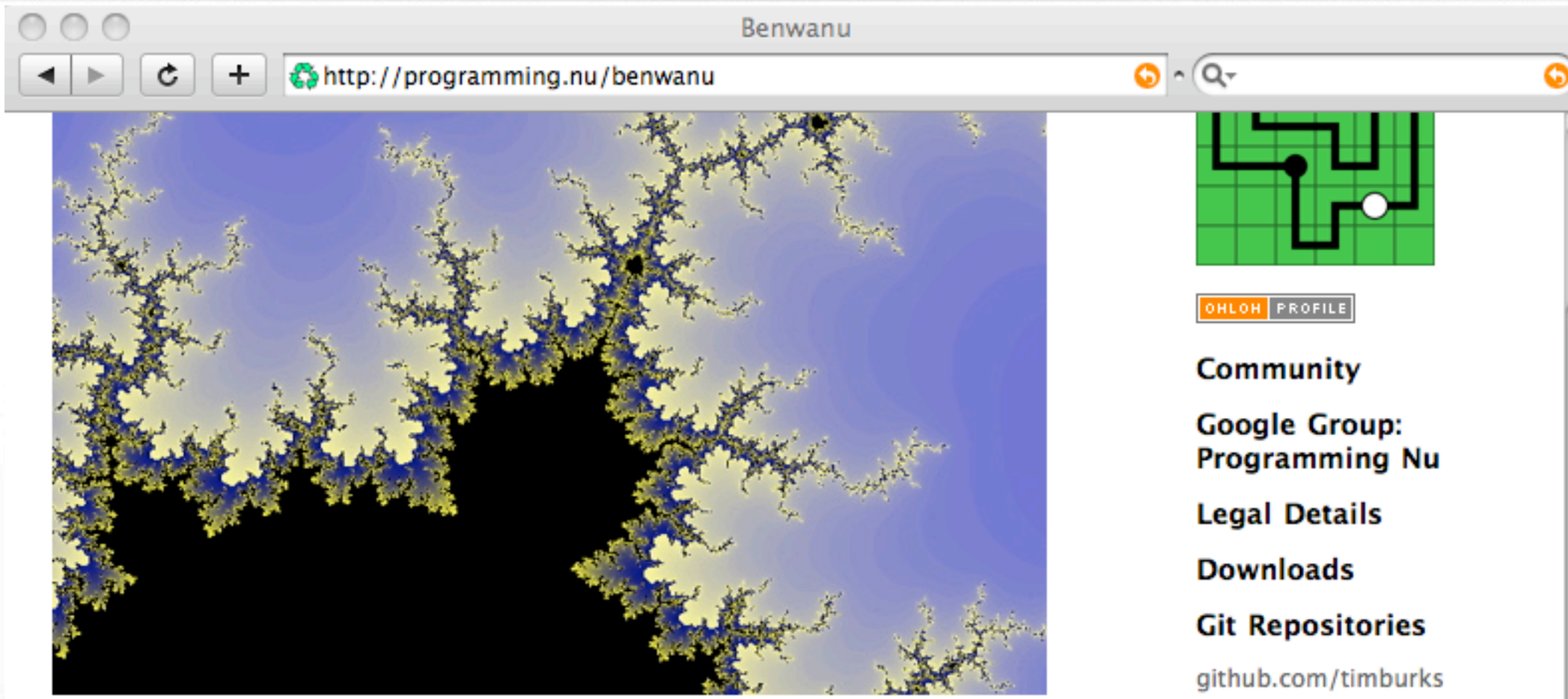
NuSAX

Adam Solove, Jonathan Yeddidia, Stephen White, Elizabeth Kellner, Matt Rice,...

tim@neontology.com


timburks's cocoa-programming-with-nu at master - GitHub
git http://github.com/timburks/cocoa-programming-with-nu/tree/master
RSS
Google
github
SOCIAL CODING
Search
Browse | Guides | Advanced
timburks
17
account | profile | log out
dashboard | gists
Source
Commits
Network (4)
Fork Queue
Downloads (0)
Wiki (1)
Graphs
Admin
master
all branches
all tags
timburks / cocoa-programming-with-nu
edit
pull request
unwatch
download
27
4
Description: Examples from the new 3rd edition of Cocoa Programming for Mac OS X, ported to Nu edit
Homepage: http://programming.nu/posts/2008/05/23/cocoa-programming-with-nu edit
Public Clone URL: git://github.com/timburks/cocoa-programming-with-nu.git
Your Clone URL: git@github.com:timburks/cocoa-programming-with-nu.git
Fixed mix-up between 09_Undo/RaiseMan_A and 09_Undo/RaiseMan_B.
jsyedidia (author)
June 01, 2008
commit bdbfd5bcadb09b6561503769
tree a4c84c13069ed41f8762b15d
parent 6c225a8c1cbed4a1e37b0ebb
cocoa-programming-with-nu /
name
age
message
.gitignore
June 01, 2008
Completed conversion of 09_Undo. [jsyedidia]
01_NuWhatIsIt/
May 23, 2008
Speakline example [Adam Solove]
02_LetsGetStarted/
May 23, 2008
Removing unnecessary files [Adam Solove]
05_TargetAction/
May 23, 2008
Speakline example [Adam Solove]

COCOA® PROGRAMMING FOR MAC® OS X
THIRD EDITION
AARON HILLEGASS



OHLOH PROFILE

Community

Google Group: Programming Nu

Legal Details

Downloads

Git Repositories

Git Repositories

github.com/timburks
code.neontology.com

News

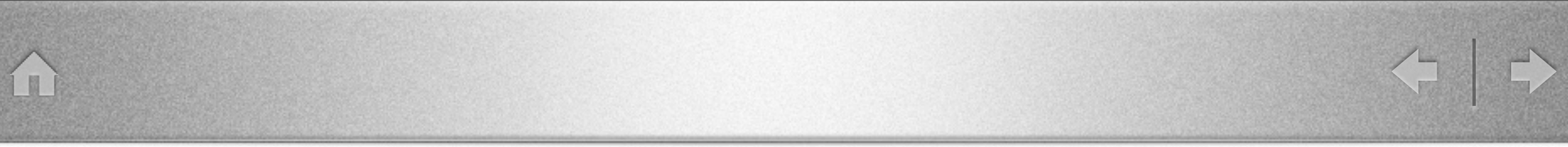
January 2009
Macros
December 2008
Nu-0.3.3
June 2008
Nu-0.3.2
May 2008
Cocoa Programming with Nu
March 2008
Nu-0.3.1
Announcing Nu: The Video
Nu on github

Benwanu

Scripting Native Threads with Nu

Benwanu is named after Benoit Mandelbrot, the discoverer of the Mandelbrot Set. Benwanu generates images of the Mandelbrot set. Its renderings follow the one Mandelbrot used in his 1982 book, The Fractal Geometry of Nature.

Benwanu demonstrates that Nu can be used to script multiple concurrent process threads (can your favorite scripting language do that?... today?).



neontology

http://blog.neontology.com/articles/page/2

RSS

Google

neontology

Learned something new today?

Nu, GNUstep, and Debian Linux

Sunday, 14 Dec 2008

I have an experimental Debian package that contains a Nu interpreter built for Debian Etch (4.0). This Nu is built to use the GNU Objective-C runtime and GNUstep-base, the GNUstep open-source equivalent of Apple's Foundation classes.

With GNUstep support, "NuFound" (aka libFoundation) support is dropped. GNUstep is actively maintained and adds at least one very important feature (UTF-8 support) that is missing in libFoundation.

All source code changes for this build are now in my Nu github repository and I will soon also add a nuke task to build the Debian package.

Please be aware that this is very new. So far it has only been tested in a VMware image, but because it is based completely on stock Debian components, I think it will hold up well.

A link and more details are below.

About this site

I'm Tim Burks,
a software developer in
Northern California.

Tools that I use

twitter.com/timburks
del.icio.us/timburks
github.com/timburks
facebook.com/timburks
linkedin.com/in/timburks
meetup.com: Silicon Valley

nu/main.nu at 978fffaaff343d584ad503547f2ff360a256eb68 from timburks's thenupill - GitHub

git http://github.com/timburks/thenupill/blob/978fffaaff343d584ad503547f2ff360a256eb68 RSS

```
215         (if (eq (nameString length) 0)
216             (set nameString "Nubie"))
217         (@label setText:(+ "Hello, " nameString "!"))))
218
219 (class ApplicationDelegate is NSObject
220      (ivars)
221      (ivar-accessors)
222
223      (- (void)applicationDidFinishLaunching:(id)application is
224         ;; Set up the window and content view
225         (set screenRect ((UIScreen mainScreen) bounds))
226         (set @window ((UIWindow alloc) initWithFrame:screenRect))
227         (set @helloViewController ((HelloViewController alloc) init))
228         (set @navigationController ((UINavigationController alloc) initWithRootViewController:@helloViewController))
229         (@window setContentView:(@navigationController view))
230
231         ;; start the server
232         (set $server ((RemoteNuServer alloc) initWithName:"Nu Server"))
233
234         ;; Show the window
235         (@window makeKeyAndVisible)))
236
237 (puts "Nu code loaded")
238
239
240
241
```

tim@neontology.com

I Jailbroke my iPhone

tim@neontology.com

What is it doing?

1. "pwning" disables signature checks in the iPhone bootloader.
2. A custom "IPSW" (iPhone Software image) disables kernel restrictions on user processes.

tim@neontology.com

planetbeing's xpwn at master – GitHub

git http://github.com/planetbeing/xpwn/tree/master RSS Google

github SOCIAL CODING

Search

Browse | Guides | Advanced

timburks

17

account | profile | log out

dashboard | gists

Source | Commits | Network (26) | Downloads (0) | Wiki (2) | Graphs

master | all branches | all tags

planetbeing / xpwn

fork | watch | download

51 | 26

Description: A cross-platform custom NOR firmware loader and custom IPSW generator for the iPhone

Homepage: http://planetbeing.lighthouseapp.com/projects/15246-xpwn

Public Clone URL: git://github.com/planetbeing/xpwn.git

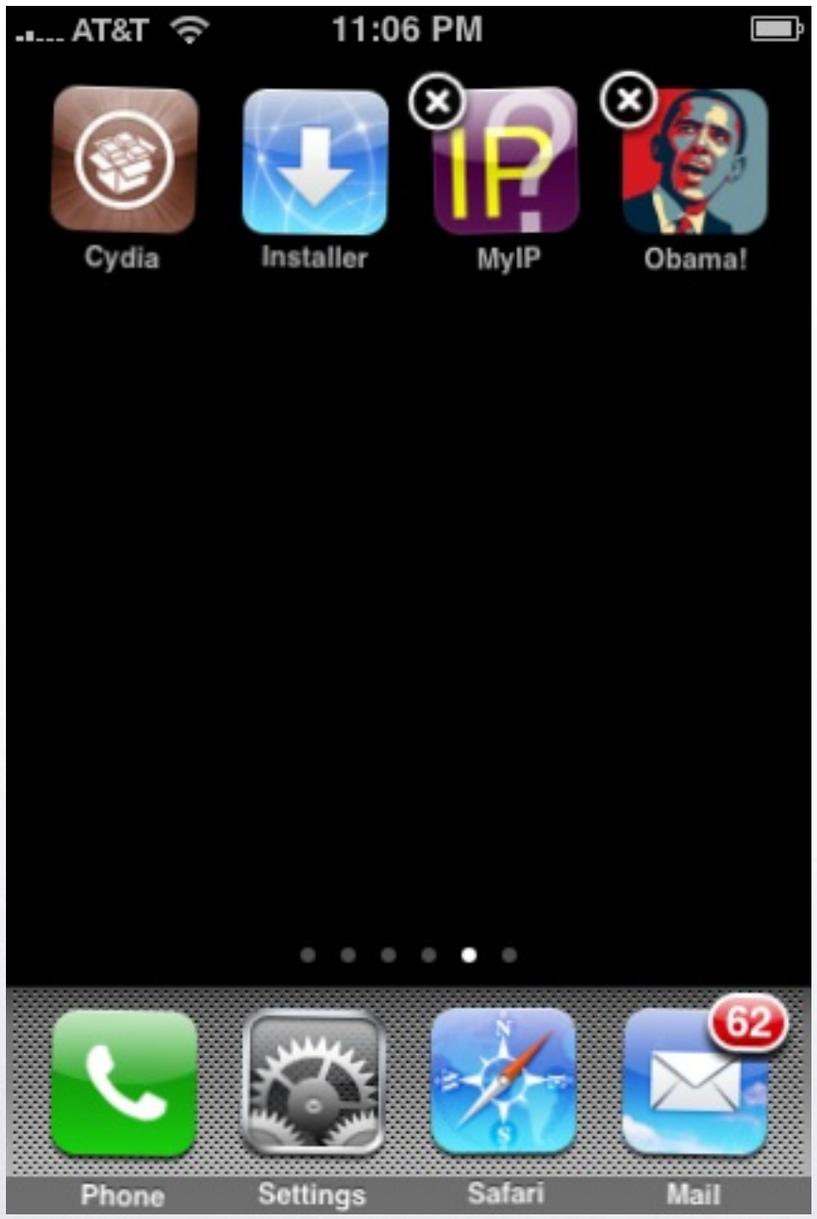
```
Made default partition size 500 MB for 2.2.1
```

planetbeing (author)
January 30, 2009

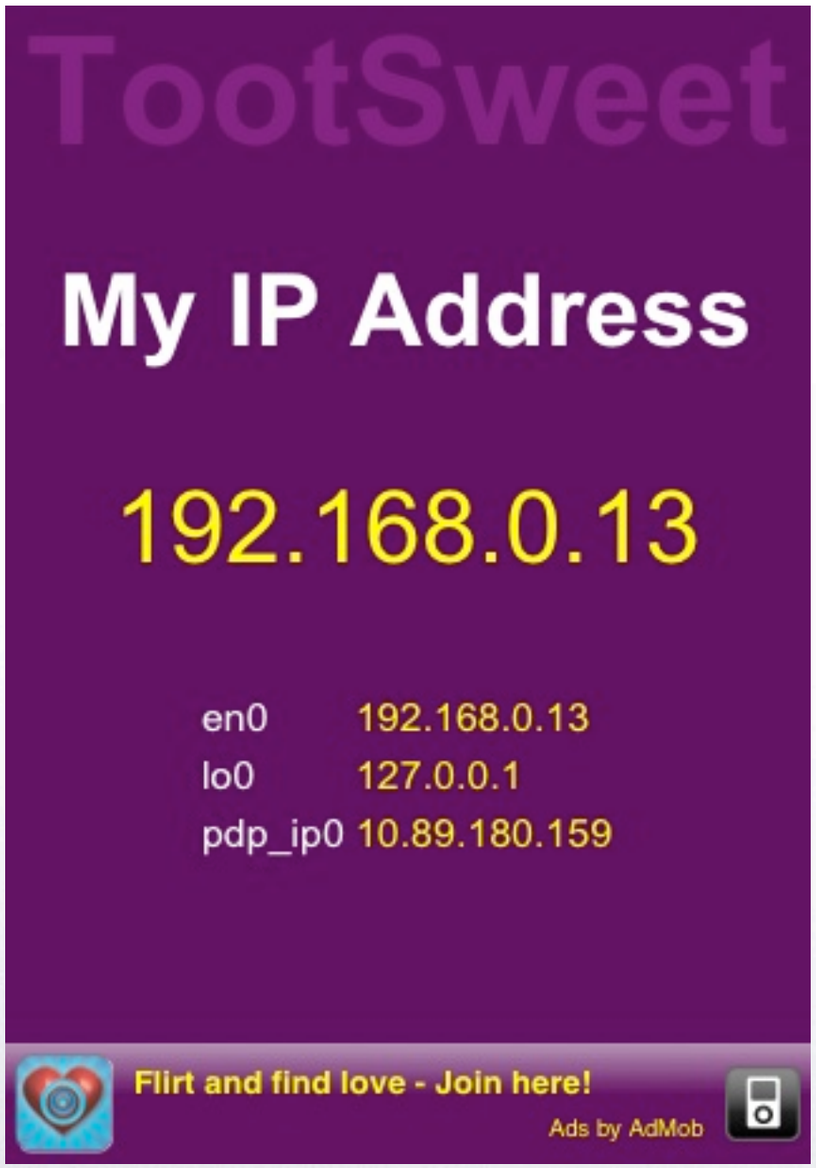
```
commit  f23cc992df9ab6771d1dcdebfb08a0e65d667b10
tree    dc02d06697bae30a366e55597a3f38ce59d25568
parent  87699cfade80a91a4ef64f6e8a3edcb9663e4085
```

xpwn /

Essentials



tim@neontology.com




```
% ssh 192.168.0.13 -l root
The authenticity of host '192.1
can't be established.
RSA key fingerprint is af:94:ba
19:63:47:97:df:f0:6f:b6:31.
Are you sure you want to continu
yes
Warning: Permanently added '192                    e
list of known hosts.
root@192.168.0.13's password:
iPhone:~ root# passwd
Changing password for root.
New password:
Retype new password:
iPhone:~ root# apt-get install vim
...

iPhone:~ root# apt-get install gdb
...

iPhone:~ root# apt-get install rsync
...
```

Out of the box, every iPhone's root password is "alpine." After you've installed OpenSSH, Change yours ASAP!

```
#rsync -avz -e ssh / me@my-machine:/myiphone
```


tim@neontology.com

```
[/myiphone] tim% cat ./private/var/stash/share.GYYNXs/sandbox/SandboxTemplate.sb
```


tim@neontology.com

```
[/myiphone] tim% find . -name "*.db"
./Library/Application Support/BTServer/pincode_defaults.db
./private/var/Keychains/keychain-2.db
./private/var/mobile/Applications/ED85406C-B7D7-427A-9865-70AF5FFDDD6C/Documents/667316288.db
./private/var/mobile/Library/CallHistory/call_history.db
./private/var/mobile/Library/Notes/notes.db
./private/var/mobile/Library/SMS/sms.db
./private/var/mobile/Library/Voicemail/voicemail.db
./private/var/mobile/Library/WebKit/Databases/Databases.db
./private/var/mobile/Library/WebKit/Databases/http_mail.google.com_0/0000000000000001.db
./System/Library/PrivateFrameworks/AppSupport.framework/calldata.db

[/myiphone] tim% find . -name "*.sqlitedb"
./private/var/mobile/Library/AddressBook/AddressBook.sqlitedb
./private/var/mobile/Library/AddressBook/AddressBookImages.sqlitedb
./private/var/mobile/Library/Caches/MapTiles/MapTiles.sqlitedb
./private/var/mobile/Library/Calendar/Calendar.sqlitedb
./private/var/root/Library/AddressBook/AddressBook.sqlitedb
./private/var/root/Library/Calendar/Calendar.sqlitedb
```

```
[/myiphone] tim% sqlite3 ./private/var/mobile/Library/CallHistory/call_history.db
SQLite version 3.5.9
Enter ".help" for instructions
sqlite> .dump
BEGIN TRANSACTION;
CREATE TABLE _SqliteDatabaseProperties (key TEXT, value TEXT, UNIQUE(key));
INSERT INTO "_SqliteDatabaseProperties" VALUES('call_history_limit','100');
INSERT INTO "_SqliteDatabaseProperties" VALUES('timer_last','60');
INSERT INTO "_SqliteDatabaseProperties" VALUES('timer_outgoing','88020');
INSERT INTO "_SqliteDatabaseProperties" VALUES('timer_incoming','76320');
INSERT INTO "_SqliteDatabaseProperties" VALUES('timer_all','164340');
INSERT INTO "_SqliteDatabaseProperties" VALUES('timer_lifetime','164340');
INSERT INTO "_SqliteDatabaseProperties" VALUES('timer_last_reset','0');
INSERT INTO "_SqliteDatabaseProperties" VALUES('data_up_last','0.5859375');
INSERT INTO "_SqliteDatabaseProperties" VALUES('data_down_last','1.380859375');
INSERT INTO "_SqliteDatabaseProperties" VALUES('data_up_all','207434.788086272');
INSERT INTO "_SqliteDatabaseProperties" VALUES('data_down_all','1946836.91406457');
INSERT INTO "_SqliteDatabaseProperties" VALUES('data_up_lifetime','207434.788086272');
INSERT INTO "_SqliteDatabaseProperties" VALUES('data_down_lifetime','1946836.91406457');
INSERT INTO "_SqliteDatabaseProperties" VALUES('data_last_reset','0');
INSERT INTO "_SqliteDatabaseProperties" VALUES('_ClientVersion','3');
INSERT INTO "_SqliteDatabaseProperties"
VALUES('_UniqueIdentifier','C1253CD2-8310-4E04-9463-7CCF6FB8D49A');
INSERT INTO "_SqliteDatabaseProperties" VALUES('__CPRecordSequenceNumber','1634');
CREATE TABLE call (ROWID INTEGER PRIMARY KEY AUTOINCREMENT, address TEXT, date INTEGER,
duration INTEGER, flags INTEGER, id INTEGER);
INSERT INTO "call" VALUES(1404,'6505551212',1233452885,60,5,638);
INSERT INTO "call" VALUES(1405,'8006332152',1233518067,60,5,638);
```

```
[/myiphone] tim% sqlite3 ./private/var/mobile/Library/Notes/notes.db
SQLite version 3.5.9
Enter ".help" for instructions
sqlite> .dump
BEGIN TRANSACTION;
CREATE TABLE _SqliteDatabaseProperties (key TEXT, value TEXT, UNIQUE(key));
INSERT INTO "_SqliteDatabaseProperties" VALUES('_ClientVersion','3');
INSERT INTO "_SqliteDatabaseProperties" VALUES('_UniqueIdentifier','CAFDFC2D-87D7-4F8A-
AC8F-C2C6561D842E');
INSERT INTO "_SqliteDatabaseProperties" VALUES('__CPRecordSequenceNumber','65');
CREATE TABLE note_bodies (note_id INTEGER, data, UNIQUE(note_id));
INSERT INTO "note_bodies" VALUES(1,'Shopping<div> </div><div><div>Bike seat</
div><div>Quick release (2)</div><div><br class="webkit-block-placeholder"></
div><div>Lightbulbs</div><div>7 frame hNgers</div><div>2wire hangers</div><div>2 screw
pairs</div><div><br class="webkit-block-placeholder"></div><div>Hand broom</
div><div>Stainless steel spray ZEP</div><div><br class="webkit-block-placeholder"></
div></div>');
INSERT INTO "note_bodies" VALUES(3,'Whirlpool et20nkxan04 door shelf bracket');
```

Finding things

- find
- grep
- nm
- strings
- otool

tim@neontology.com

```
[/myiphone] tim% cd System/Library/PrivateFrameworks

[System/Library/PrivateFrameworks] tim% find . -exec grep Battery {} \;
Binary file ./BluetoothManager.framework/BluetoothManager matches
Binary file ./CoreTelephony.framework/CoreTelephony matches
Binary file ./CoreTelephony.framework/Support/CommCenter matches
Binary file ./IAP.framework/IAP matches
Binary file ./IAP.framework/Support/iapd matches
Binary file ./MobileBluetooth.framework/MobileBluetooth matches
Binary file ./SpringBoardServices.framework/SpringBoardServices matches
grep: ./WebKit.framework/Frameworks: No such file or directory

[System/Library/PrivateFrameworks] tim% cd CoreTelephony.framework/

[Library/PrivateFrameworks/CoreTelephony.framework] tim% ls
CoreTelephony English.lproj Info.plist    Support

[Library/PrivateFrameworks/CoreTelephony.framework] tim% strings CoreTelephony | grep Battery
kCTIndicatorsBatteryCapacity
kCTIndicatorsBatteryCapacityNotification

[Library/PrivateFrameworks/CoreTelephony.framework] tim% nm CoreTelephony | grep Battery
31be15c4 T _CTGetBatteryCapacity
31be83a4 T __CTGetBatteryCapacity
31be14fc T __CTIndicatorsHandleBatteryCapacityNotification
31bee99a T __CTServerConnectionGetBatteryCapacity
39bdcae4 S _kCTIndicatorsBatteryCapacity
39bdcae8 S _kCTIndicatorsBatteryCapacityNotification
```


tim@neontology.com

otool

Display load commands with
otool -l <file>

Display shared library dependencies with
otool -L <file>

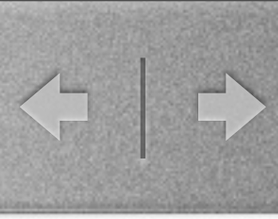
Dissassemble with
otool -tV <file>

Display Objective-C tables with
otool -o <file>

“man otool” for more.

```
_CTGetBatteryCapacity:
31be15c4            b5f0        push    {r4, r5, r6, r7, lr}
31be15c6            af03        add     r7, sp, #12
31be15c8            b084        sub     sp, #16
31be15ca            2300        mov     r3, #0
31be15cc            9302        str     r3, [sp, #8]
31be15ce        feb7f7ff        bl      _CTTelephonyCenterGetDefault
31be15d2            1c06        mov     r6, r0              (add r6, r0, #0)
31be15d4            3608        add     r6, #8
31be15d6            1c05        mov     r5, r0              (add r5, r0, #0)
31be15d8            1c30        mov     r0, r6              (add r0, r6, #0)
31be15da        eb5af017        blx     0x31bf8c90          ; symbol stub for: _pthread_mutex_lock
31be15de            466b        mov     r3, sp
31be15e0            4668        mov     r0, sp
31be15e2            6b69        ldr     r1, [r5, #52]
31be15e4            aa02        add     r2, sp, #8
31be15e6            330f        add     r3, #15
31be15e8        f9d7f00d        bl      __CTServerConnectionGetBatteryCapacity
31be15ec            9c01        ldr     r4, [sp, #4]
31be15ee            1c30        mov     r0, r6              (add r0, r6, #0)
31be15f0        eb56f017        blx     0x31bf8ca0          ; symbol stub for: _pthread_mutex_unlock
31be15f4            2c00        cmp     r4, #0
31be15f6            d002        beq     0x31be15fe
31be15f8            1c28        mov     r0, r5              (add r0, r5, #0)
31be15fa        fdc9f7ff        bl      __CTTelephonyCenterReEstablishServerConnection
31be15fe            9802        ldr     r0, [sp, #8]
31be1600            b004        add     sp, #16
31be1602            bdf0        pop     {r4, r5, r6, r7, pc}
```


tim@neontology.com

Learn Assembly with gcc

```
tim% man gcc
GCC(1)                                  GNU                                  GCC(1)

NAME
       gcc - GNU project C and C++ compiler

SYNOPSIS
       gcc [-c|-S|-E] [-std=standard]
           [-g] [-pg] [-Olevel]
           [-Wwarn...] [-pedantic]
           [-Idir...] [-Ldir...]
           [-Dmacro[=defn]...] [-Umacro]
           [-foption...] [-mmachine-option...]
           [-o outfile] infile...

...

       -S  Stop after the stage of compilation proper; do not assemble.  The
           output is in the form of an assembler code file for each non-
           assembler input file specified.

           By default, the assembler file name for a source file is made by
           replacing the suffix .c, .i, etc., with .s.
```


tim@neontology.com

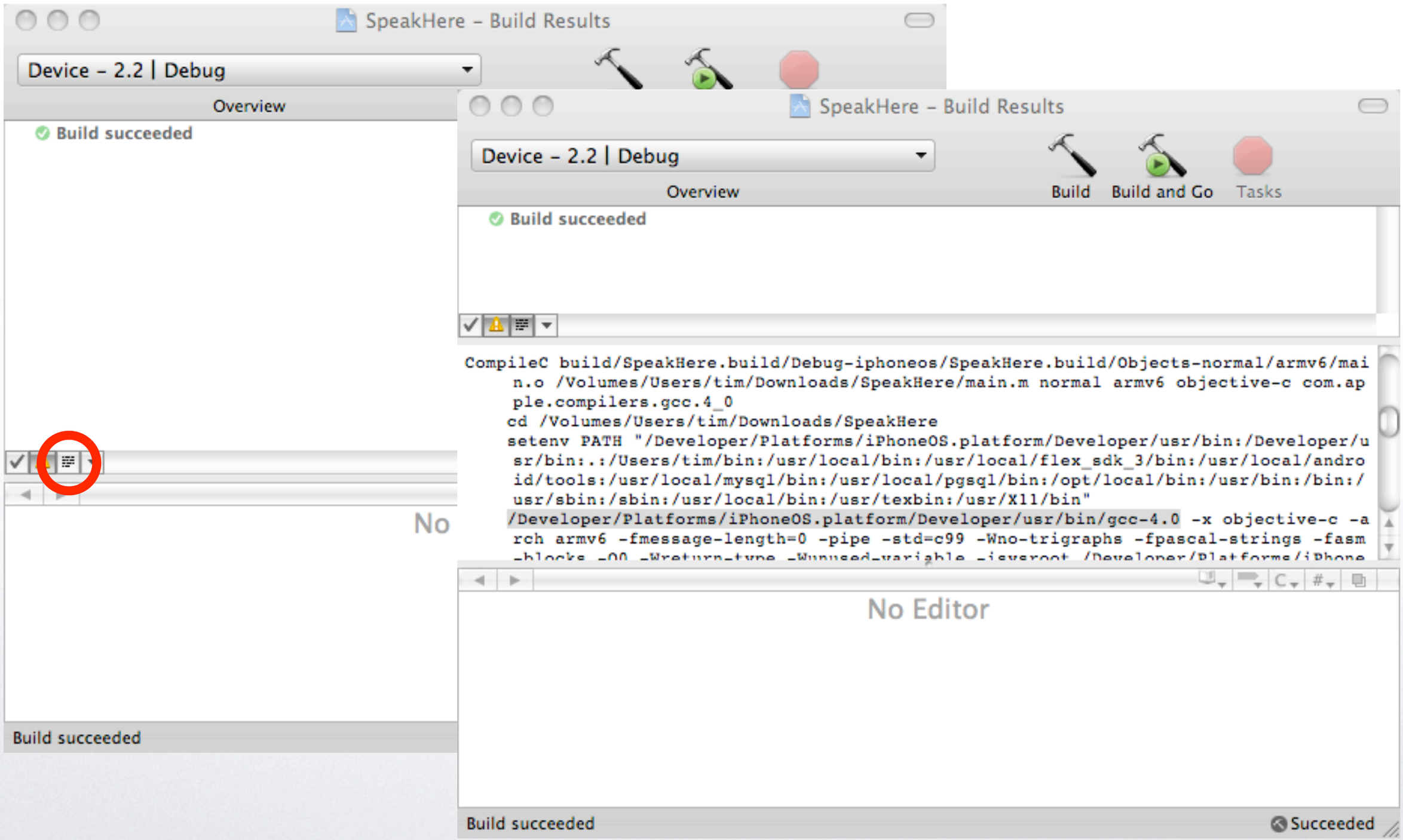
```
tim% cat sample.c

int multiply_add(int a, int b, int c) {
  return a*b + c;
}

tim% gcc sample.c -S

tim% cat sample.s
    .text
.globl _multiply_add
_multiply_add:
    pushl   %ebp
    movl    %esp, %ebp
    subl    $8, %esp
    movl    8(%ebp), %eax
    imull   12(%ebp), %eax
    addl    16(%ebp), %eax
    leave
    ret
    .subsections_via_symbols

tim% gcc sample.c -S -arch armv6
gcc-4.0: installation problem, cannot exec '/usr/bin/arm-apple-darwin9-gcc-4.0.1':
No such file or directory
```


SpeakHere – Build Results
Device – 2.2 | Debug
Overview
Build succeeded
SpeakHere – Build Results
Device – 2.2 | Debug
Build
Build and Go
Tasks
Overview
Build succeeded
CompileC build/SpeakHere.build/Debug-iphoneos/SpeakHere.build/Objects-normal/armv6/main.o /Volumes/Users/tim/Downloads/SpeakHere/main.m normal armv6 objective-c com.apple.compilers.gcc.4_0
cd /Volumes/Users/tim/Downloads/SpeakHere
setenv PATH "/Developer/Platforms/iPhoneOS.platform/Developer/usr/bin:/Developer/usr/bin:.:/Users/tim/bin:/usr/local/bin:/usr/local/flex_sdk_3/bin:/usr/local/android/tools:/usr/local/mysql/bin:/usr/local/pgsql/bin:/opt/local/bin:/usr/bin:/bin:/usr/sbin:/sbin:/usr/local/bin:/usr/texbin:/usr/X11/bin"
/Developer/Platforms/iPhoneOS.platform/Developer/usr/bin/gcc-4.0 -x objective-c -arch armv6 -fmessage-length=0 -pipe -std=c99 -Wno-trigraphs -fpascal-strings -fasm
No
No Editor
Build succeeded
Build succeeded
Succeeded

```
tim% /Developer/Platforms/iPhoneOS.platform/Developer/usr/bin/gcc-4.0 sample.c -S -arch armv6
```

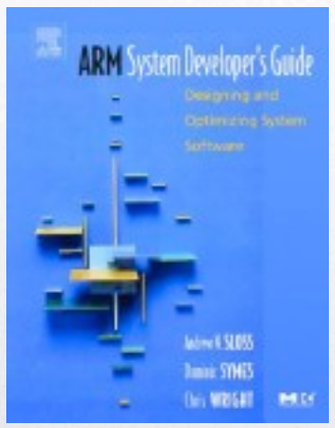
```
tim% cat sample.s
     .text
     .align 2
     .globl _multiply_add
_multiply_add:
     @ args = 0, pretend = 0, frame = 12
     @ frame_needed = 1, uses_anonymous_args = 0
     stmfd     sp!, {r7, lr}
     add  r7, sp, #0
     sub  sp, sp, #12
     str  r0, [sp, #8]
     str  r1, [sp, #4]
     str  r2, [sp, #0]
     ldr  r2, [sp, #8]
     ldr  r3, [sp, #4]
     mul  r2, r3, r2
     ldr  r3, [sp, #0]
     add  r3, r2, r3
     mov  r0, r3
     sub  sp, r7, #0
     ldmfd     sp!, {r7, pc}
```

```
int multiply_add(int a, int b, int c) {
  return a*b + c;
}
```

```
tim% /Developer/Platforms/iPhoneOS.platform/Developer/usr/bin/gcc-4.0 sample.c -S -arch armv6 -O

tim% cat sample.s
     .text
     .align 2
     .globl _multiply_add
_multiply_add:
     @ args = 0, pretend = 0, frame = 0
     @ frame_needed = 0, uses_anonymous_args = 0
     @ link register save eliminated.
     @ lr needed for prologue
     mla  r0, r1, r0, r2
     bx   lr
     .subsections_via_symbols
```

```
int multiply_add(int a, int b, int c) {
  return a*b + c;
}
```



MLA — Multiply with accumulate

1. MLA<cond>{S} Rd, Rm, Rs, Rn — ARMv2

Action	Effect on the *cpsr*
1. Rd = Rn + Rm*Rs	Updated if S suffix supplied

- ARM System Developer's Guide, Sloss, Symes, Wright, & Rayfield


Dynamically load functions with libdl

```
#include <dlfcn.h>

...

// Dynamically load library with this:
void *handle = dlopen("/System/Library/PrivateFrameworks/CoreTelephony.framework/CoreTelephony",
                      RTLD_LOCAL | RTLD_LAZY);
// or this:
[[NSBundle bundleWithPath:@"/System/Library/PrivateFrameworks/CoreTelephony.framework"] load];
```

```
...

// Lookup desired function with this:
int (*myGetBatteryCapacity)() = dlsym(handle, "CTGetBatteryCapacity");
// or this:
int (*myGetBatteryCapacity)() = dlsym(RTLD_DEFAULT, "CTGetBatteryCapacity");


...

// Call imported function
int capacity = myGetBatteryCapacity ? myGetBatteryCapacity() : -1;
```


tim@neontology.com

otool and Objective-C

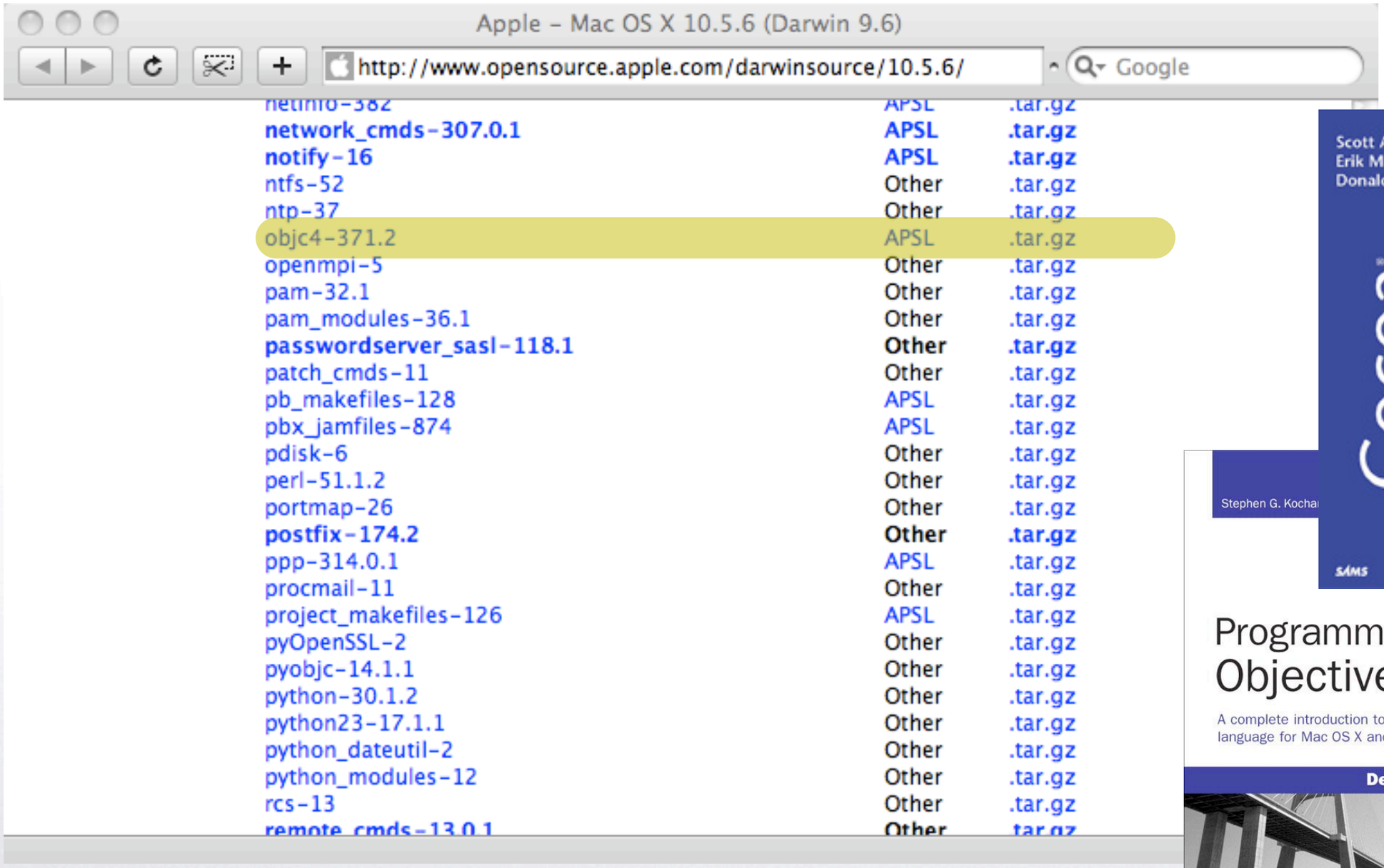
tim@neontology.com

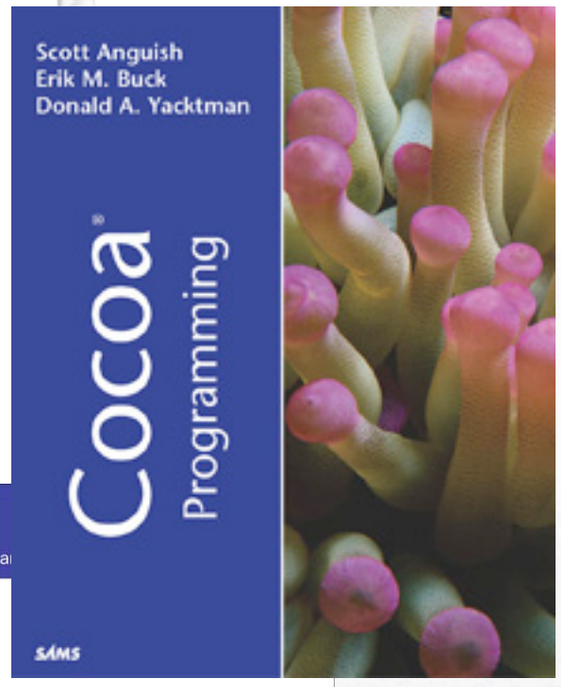
```
[Oxygen:Library/Frameworks/CoreLocation.framework] tim% otool -o CoreLocation
CoreLocation:
          Contents of (__DATA,__objc_classlist) section
39579d98 0x3957914c
            isa 0x39579188
     superclass 0x3823a6f8
          cache 0x301a7f08
         vtable 0x380bb234
           data 0x39579160 (struct class_ro_t *)
                    flags 0x0
              instanceStart 4
               instanceSize 8
                 ivarLayout 0x0
                       name 0x31581290 CLLocation
                baseMethods 0x39579220 (struct method_list_t *)
               entsize 12
                 count 18
                  name 0x3158108c getDistanceFrom:
                 types 0x31580f30 d12@0:4r@8
                   imp 0x3157de60
                  name 0x31580de0 course
                 types 0x31580f3c d8@0:4
                   imp 0x3157de34
                  name 0x31580df0 speed
                 types 0x31580f3c d8@0:4
                   imp 0x3157de08
                  name 0x31580df8 heading
                 types 0x31580f3c d8@0:4
                   imp 0x3157dddc
                  name 0x31580e00 clientLocation
                 types 0x31580f44 {?=i{?=dd}ddddddd}8@0:4
                   imp 0x3157dda0
```

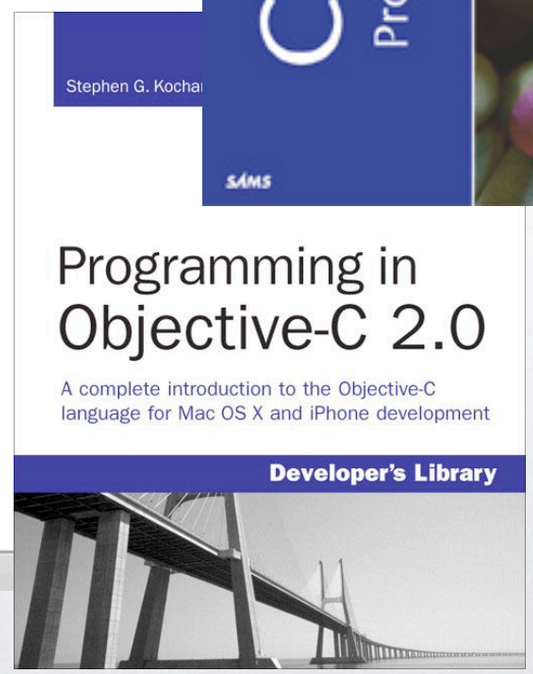
```
% cd /usr/include/objc/
[Xenon-3:/usr/include/objc] tim% ls
List.h          malloc.h          objc-load.h
Object.h        message.h         objc-runtime.h
Protocol.h      objc-api.h        objc-sync.h
error.h         objc-auto.h       objc.h
hashtable.h     objc-class.h      runtime.h
hashtable2.h    objc-exception.h  zone.h

[Xenon-3:/usr/include/objc] tim% grep IMP *
...
objc.h:typedef id          (*IMP)(id, SEL, ...);
```


tim@neontology.com







tim@neontology.com


```
iPhone:~ root# nush
Nu Shell.
Cannot read termcap database;
using dumb terminal settings.

% (load "CoreLocation")
t

% (puts ((CLLocation instanceMethodNames) description))
(
    altitude,
    clientLocation,
    coordinate,
    "copyWithZone:",
    course,
    dealloc,
    description,
    "encodeWithCoder:",
    "getDistanceFrom:",
    heading,
    horizontalAccuracy,
    "initWithClientLocation:",
    "initWithCoder:",
    "initWithCoordinate:altitude:horizontalAccuracy:verticalAccuracy:timestamp:",
    "initWithLatitude:longitude:",
    speed,
    timestamp,
    verticalAccuracy
)
()
```


```
% (CLLocationManager instanceMethodWithName:"supportInfo")
<NuMethod:31b570>

% ((CLLocationManager instanceMethodWithName:"supportInfo") signature)
"c@:"

% ((CLLocation alloc) init)
<CLLocation:31bd50>

% (((CLLocation alloc) init) description)
Bus error

iPhone:~ root# nush
Nu Shell.
Cannot read termcap database;
using dumb terminal settings.

% ((CLLocation alloc) init)
NuUndefinedSymbol: undefined symbol: CLLocation

% (load "CoreLocation")
t

% ((CLLocation alloc) init)
<CLLocation:31bd50>

% (class CLLocation (- description is "your house"))
()

% (((CLLocation alloc) init) description)
"your house"
```


tim@neontology.com


```
iPhone:~ root# cat battery.nu
#!/bin/nush

(set NSUTF8StringEncoding 4)

(set b (NSBundle bundleWithPath:"/System/Library/PrivateFrameworks/CoreTelephony.framework"))
(b load)

(set capacity (NuBridgedFunction functionWithName:"CTGetBatteryCapacity" signature:"i"))
(set sleep (NuBridgedFunction functionWithName:"sleep" signature:"ii"))

(function append-to-file (filename text)
    (unless ((NSFileManager defaultManager) fileExistsAtPath:filename)
        ((NSFileManager defaultManager) createFileAtPath:filename contents:nil attributes:nil))
    (set handle (NSFileHandle fileHandleForWritingAtPath:filename))
    (handle seekToEndOfFile)
    (handle writeData:((+ text "\n") dataUsingEncoding:NSUTF8StringEncoding))
    (handle closeFile))

(while YES
  (set c (capacity))
  (if (eq c 0) (set c (capacity))) ;; sometimes we have to retry to get a nonzero value
  (set measurement (+ ((NSDate date) description) "," c))
  (append-to-file "/var/root/battery.log" measurement)
  (sleep 120))
```

```
iPhone:~ root# tail battery.log
2009-03-01 23:22:49 -0800,78
2009-03-01 23:24:49 -0800,77
2009-03-01 23:26:49 -0800,77
2009-03-02 00:13:04 -0800,75
2009-03-02 00:28:44 -0800,75
2009-03-02 00:30:44 -0800,74
2009-03-02 00:32:44 -0800,72
2009-03-02 00:34:44 -0800,71
2009-03-02 00:45:40 -0800,71
2009-03-02 00:47:40 -0800,70
```

launchd

```
# cat /Library/LaunchDaemons/com.tootsweet.battery.plist
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
     <key>Label</key>
     <string>com.tootsweet.battery</string>
     <key>Nice</key>
     <integer>20</integer>
     <key>ProgramArguments</key>
     <array>
          <string>/var/root/battery.nu</string>
     </array>
     <key>RunAtLoad</key>
     <true/>
     <key>KeepAlive</key>
     <true/>
</dict>
</plist>
```

Build Property Lists with Nu (Mac OS)

```
tim% nush
Nu Shell.

% (set plist (NSObject readFromPropertyList:"com.tootsweet.battery.plist"))
<NSCFDictionary:24eeb0>

% (puts (plist description))
{
    KeepAlive = 1;
    Label = "com.tootsweet.battery";
    Nice = 20;
    ProgramArguments =     (
        "/var/root/battery.nu"
    );
    RunAtLoad = 1;
}
()

% (set newlist (dict Label:"com.tootsweet.battery" Nice:20 ProgramArguments:(array "/var/root/
battery.nu") KeepAlive:1 RunAtLoad:1))
<NSCFDictionary:247700>

% (newlist writeToPropertyList:"another.plist")
1
% (set newlist (dict Label:"com.tootsweet.battery" Nice:20 ProgramArguments:(array "/var/root/
battery.nu") KeepAlive:(NSNumber numberWithBool:1) RunAtLoad:(NSNumber numberWithBool:1)))
<NSCFDictionary:2411c0>
% (newlist writeToPropertyList:"yetanother.plist")
1
```


tim@neontology.com

```
tim% cat another.plist
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
     <key>KeepAlive</key>
     <integer>1</integer>
     <key>Label</key>
     <string>com.tootsweet.battery</string>
     <key>Nice</key>
     <integer>20</integer>
     <key>ProgramArguments</key>
     <array>
          <string>/var/root/battery.nu</string>
     </array>
     <key>RunAtLoad</key>
     <integer>1</integer>
</dict>
</plist>
```

```
tim% cat com.tootsweet.battery.plist
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.
<plist version="1.0">
<dict>
     <key>Label</key>
     <string>com.tootsweet.battery</string>
     <key>Nice</key>
     <integer>20</integer>
     <key>ProgramArguments</key>
     <array>
          <string>/var/root/battery.nu</string>
     </array>
     <key>RunAtLoad</key>
     <true/>
     <key>KeepAlive</key>
     <true/>
</dict>
</plist>
```


tim@neontology.com

```
% (set newlist (dict Label:"com.tootsweet.battery" Nice:20 ProgramArguments:(array "/var/root/
battery.nu") KeepAlive:(NSNumber numberWithBool:1) RunAtLoad:(NSNumber numberWithBool:1)))
<NSCFDictionary:2411c0>

% (newlist writeToPropertyList:"yetanother.plist")
1
```

```
...
<plist version="1.0">
<dict>
     <key>KeepAlive</key>
     <true/>
     <key>Label</key>
     <string>com.tootsweet.battery</string>
     <key>Nice</key>
     <integer>20</integer>
     <key>ProgramArguments</key>
     <array>
          <string>/var/root/battery.nu</string>
     </array>
     <key>RunAtLoad</key>
     <true/>
</dict>
</plist>
```

Open Radar

Open Radar

http://openradar.appspot.com/page/1

Google

Open Radar

Community bug reports

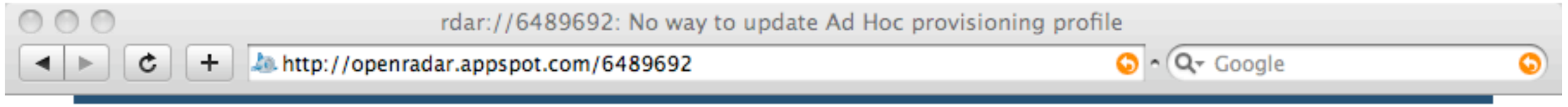
Home | Recent Comments | Sign in

Search

Page 1 next

Number	Status	Originator	Product	Title
rdar://6635276	Open	carpeaqua	iPhone SDK	Add UIKeyboard number pad with decimal point
rdar://6635063	Open	xfox	Mac OS X	Error in the Italian localization of the DiskArbitration framework
rdar://6634865	Open	joachimb	Safari	Safari 4: Have Top Sites behave like an empty page
rdar://6634756	Open	astrange	iApps	iTunes should sort added files by album if multiple albums are dragged in
rdar://6634734	Open	astrange	Safari	Better handling of pages with forms in address bar complete
rdar://6634702	Open	astrange	Safari	Safari 4: Removing link from bookmarks menu doesn't update address bar
rdar://6634655	Open	astrange	Safari	Safari 4: Allow external links to take over a Top Sites tab
rdar://6634184	Open	hweeboon	iPhone SDK	UIImage +imageNamed: is filename case-insensitive in

tim@neontology.com



Open Radar

Home | Recent Comments | Sign in

Search

Community bug reports

No way to update Ad Hoc provisioning profile

Originator:	craig.hockenberry		
Number:	rdar://6489692	Date Originated:	
Status:	Open	Resolved:	
Product:	iPhone SDK	Product Version:	
Classification:		Reproducible:	

There is no way to add a new device to an Ad Hoc provisioning profile. If I add a user for beta testing, I have to manually recreate a new profile.

In order to do this, I have to CLICK A LOT OF FUCKING CHECKBOXES.

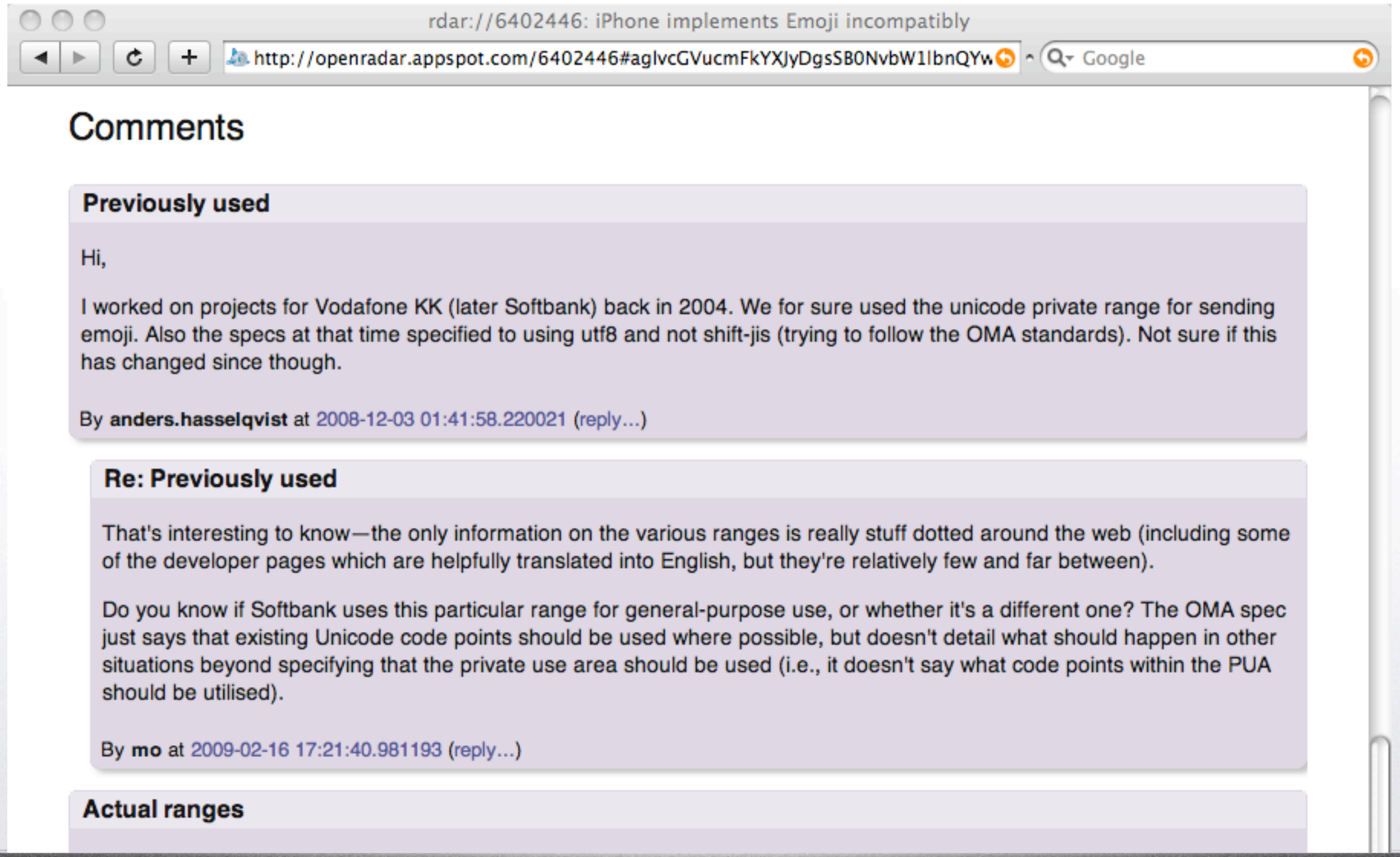
And since I have multiple products, I have to PAY ATTENTION TO WHICH OF THESE FUCKING CHECKBOXES GET CHECKED.

I know that this change was done to prevent people from distributing products using Ad Hoc profiles, but all it does is penalize the developers who are playing by the rules. And the end result is that I don't add new beta testers for our products (resulting in less testing and lower quality.)

Please deal with Ad Hoc abuse by revoking certificates, not by making the editing process more cumbersome.

12-Jan-2009 04:26 PM Craig Hockenberry:
I have my Ad Hoc profile back now. And it's not at all obvious what is causing the root of the problem.

The Distribution certificate had been removed (Program Portal > Certificates > Distribution.) That, in turn, led the Ad Hoc provision from being "invalidated" so that I could not edit it.


rdar://6402446: iPhone implements Emoji incompatibly
http://openradar.appspot.com/6402446#aglvcGVucmFkYXJyDgsSB0NvbW1lbnQYw
Google
Comments
Previously used
Hi,
I worked on projects for Vodafone KK (later Softbank) back in 2004. We for sure used the unicode private range for sending emoji. Also the specs at that time specified to using utf8 and not shift-jis (trying to follow the OMA standards). Not sure if this has changed since though.
By anders.hasselqvist at 2008-12-03 01:41:58.220021 (reply...)
Re: Previously used
That's interesting to know—the only information on the various ranges is really stuff dotted around the web (including some of the developer pages which are helpfully translated into English, but they're relatively few and far between).
Do you know if Softbank uses this particular range for general-purpose use, or whether it's a different one? The OMA spec just says that existing Unicode code points should be used where possible, but doesn't detail what should happen in other situations beyond specifying that the private use area should be used (i.e., it doesn't say what code points within the PUA should be utilised).
By mo at 2009-02-16 17:21:40.981193 (reply...)
Actual ranges

Quota Details for Open Radar

http://appengine.google.com/dashboard/quotadetails?&app_id=openradar&version_ic

open radar

Google App Engine

timburks@gmail.com | My Account | Help | Sign out

openradar **Version:** 1

« Show All Applications

Main

Dashboard

Quota Details

The quota details for this application are grouped by API and are listed below. If your application exceeds 50% of any particular quota halfway through the day, it may exceed the quota before the day is over. To learn more about how quotas work, read Understanding Quotas and Why is My App Over Quota?

Requests

Quotas are reset every 24 hours. Next reset: 4 hours

timburks's openradar at master - GitHub

git http://github.com/timburks/openradar/tree/master RSS

open radar

github SOCIAL CODING

Search

Browse | Guides | Advanced

timburks

17

account | profile | log out

dashboard | gists

Source | Commits | Graphs | Wiki (1) | Network (3) | Fork Queue | Admin

master all branches all tags

timburks / openradar edit | pull request | unwatch | download

21 3

Description: A Google App Engine app for sharing information about radars that we've submitted. edit

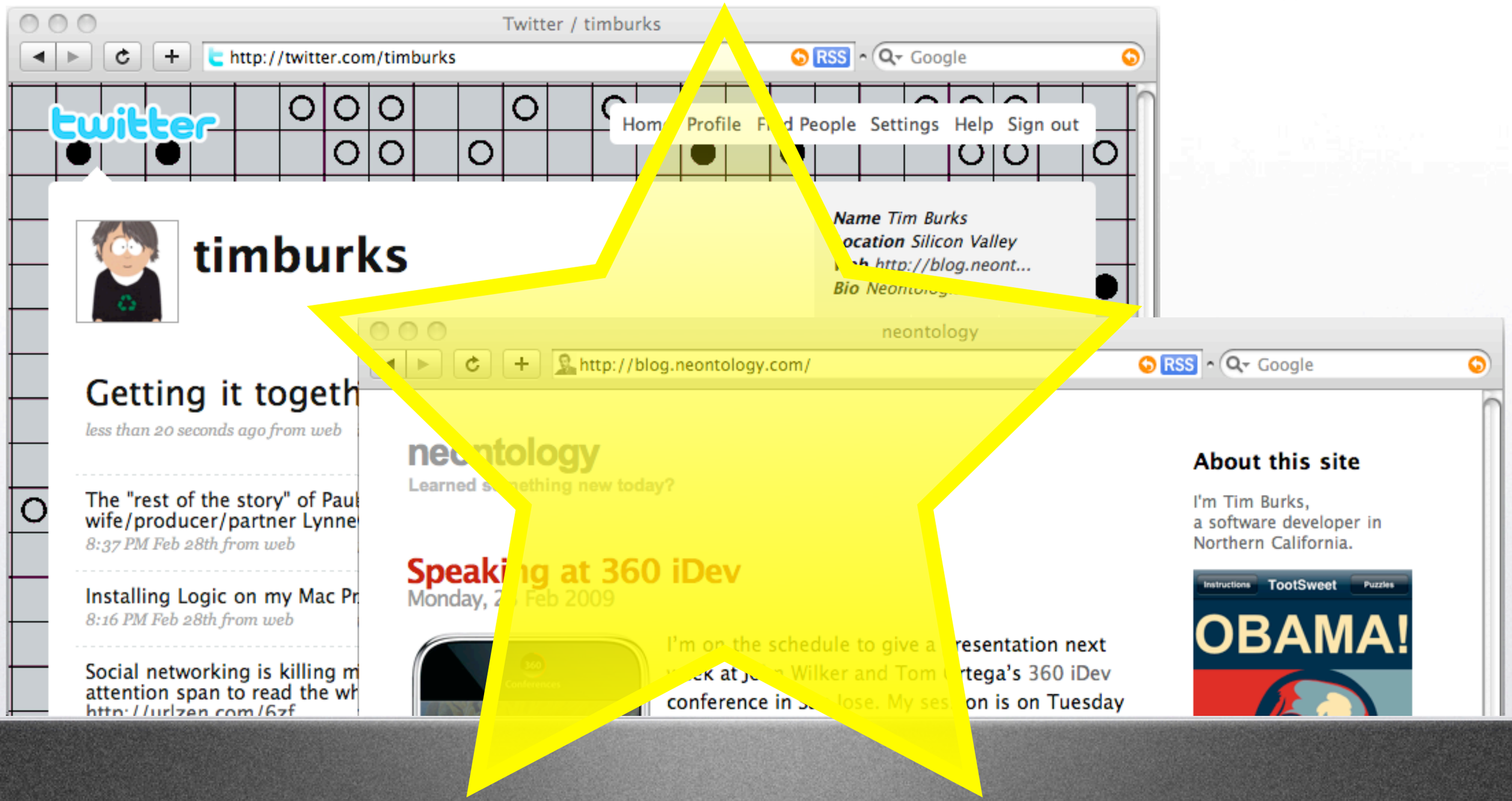
Homepage: http://openradar.appspot.com edit

Public Clone URL: git://github.com/timburks/openradar.git

Your Clone URL: git@github.com:timburks/openradar.git

tim@neontology.com

Thanks for Listening!



tim@neontology.com