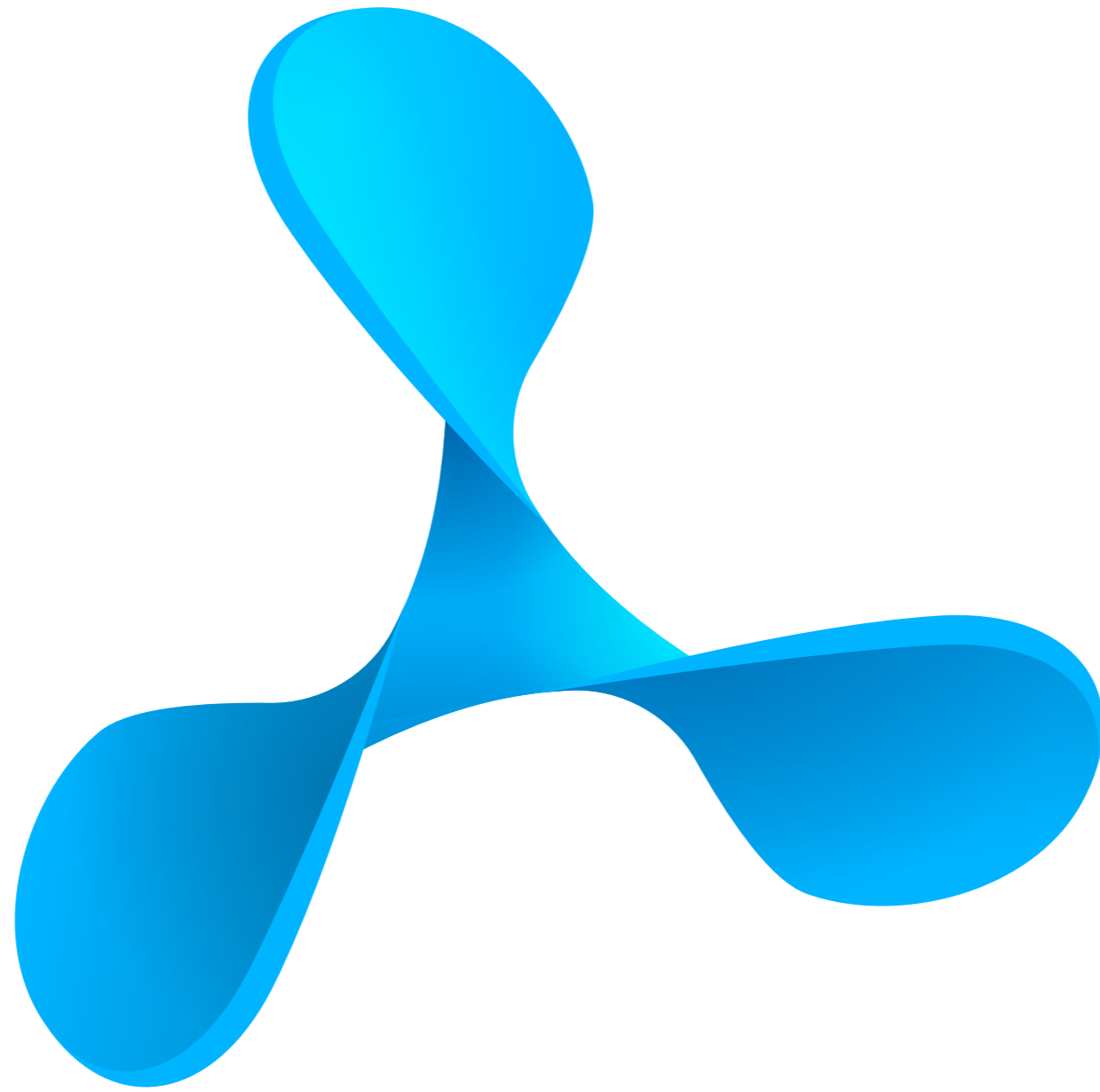


Taking Advantage of the Runtime

Peter Steinberger
@steipete

Mobile Central Europe, January 2014, Warsaw, Poland



PSPDFKit

iOS PDF Framework

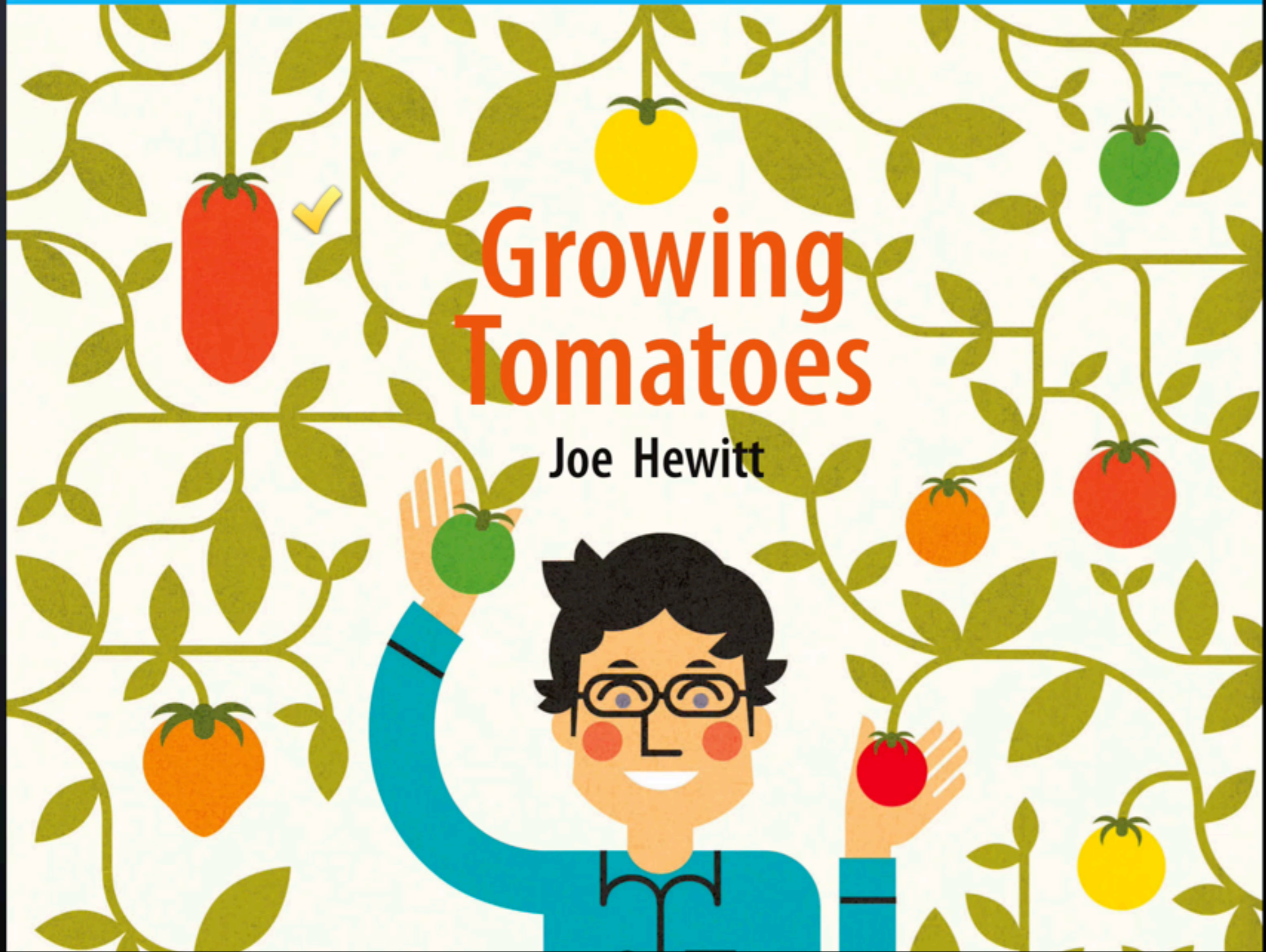
Fixing Bugs in UIKit

UIPrintViewController



Growing Tomatoes

Joe Hewitt



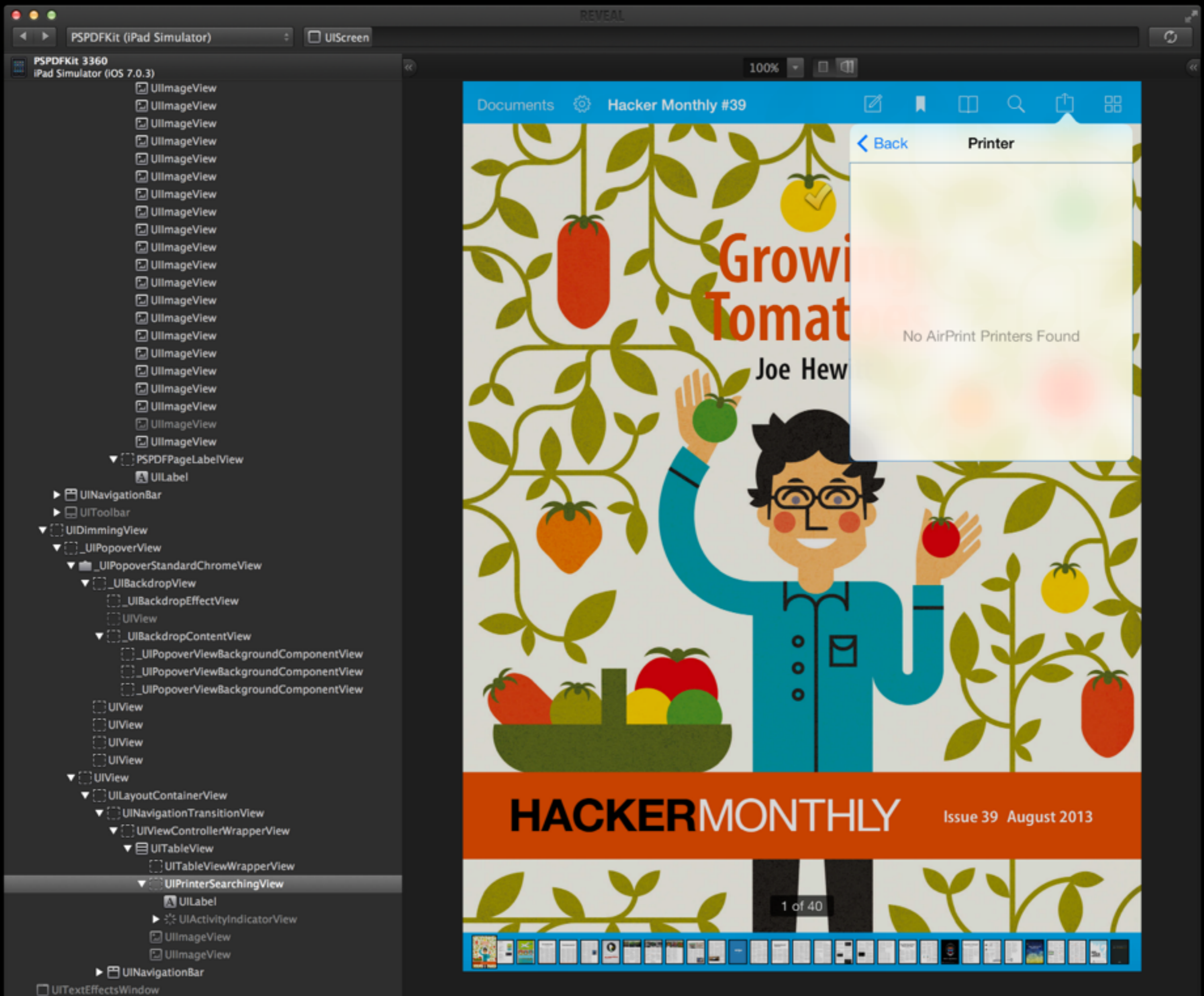


Growing Tomatoes

Joe Hewitt



UIPrintViewController





branch: master ▾

iOS-Runtime-Headers / Frameworks / UIKit.framework / UIPrinterSearchingView.h



Nicolas Seriot 11 months ago 5.0

1 contributor



file | 19 lines (14 sloc) | 0.395 kb



Open

Edit

Raw

Blame

History

Delete

```
1  /* Generated by RuntimeBrowser
2     Image: /System/Library/Frameworks/UIKit.framework/UIKit
3  */
4
5  @class UIActivityIndicatorView, UILabel;
6
7  @interface UIPrinterSearchingView : UIView {
8      UIActivityIndicatorView *_searchingIndicator;
9      UILabel *_searchingLabel;
10 }
11
12 - (void)dealloc;
13 - (id)initInView:(id)arg1;
14 - (void)layoutSubviews;
15 - (void)searchTimeout;
16 - (void)setSearching:(BOOL)arg1;
17
18 @end
```

```
UIView *searchingLabel = ViewOfClass(_self, NSStringFromClass(UILabel.class));
UIView *searchingIndicator = ViewOfClass(_self, NSStringFromClass(UIActivityIndicatorView.class));

CGRect centeredRect = AlignRectangles(searchingLabel.frame, _self.bounds, PSPDFRectAlignCenter);

CGRect searchingLabelRect = searchingLabel.frame;
searchingLabelRect.origin.y = centeredRect.origin.y;
searchingLabel.frame = searchingLabelRect;

CGRect indicatorFrame = searchingIndicator.frame;
indicatorFrame.origin.y = searchingLabel.frame.origin.y;
searchingIndicator.frame = indicatorFrame;
```

```
__attribute__((constructor)) static void FixCenteringInPrinterBrowserViewController(void) {  
    Class printerSearchingViewClass = NSClassFromString(@"UIPrinterSearchingView");  
    if (printerSearchingViewClass) {  
        SEL customLayoutSubviewsSEL = NSSelectorFromString(@"pspdf_layoutSubviews");  
        id customLayoutSubviews = ^(UIView *_self) {  
            ((void( *) (id, SEL))objc_msgSend)(_self, customLayoutSubviewsSEL); // call original.  
  
            // Call custom layouting code  
        };  
  
        ReplaceMethodWithBlock(printerSearchingViewClass, @selector(layoutSubviews),  
                               customLayoutSubviewsSEL, customLayoutSubviews);  
    }  
}
```

<http://petersteinberger.com/blog/2014/fixing-what-apple-doesnt>

```
__attribute__((constructor)) static void PSPDFFixCenteringInPrinterBrowserViewController(void) {  
    Class printerSearchingViewClass = NSClassFromString([NSString stringWithFormat:@"UI%@Searching%@", @"Printer", @"View"]);  
    if (printerSearchingViewClass) {  
        SEL customLayoutSubviewsSEL = PSPDFPrefixedSelector(layoutSubviews);  
        id customLayoutSubviews = ^(UIView *_self) {  
            ((void( *)(id, SEL))objc_msgSend)(_self, customLayoutSubviewsSEL); // call original.  
            @try {  
                if ([PSPDFIsUIKitFlatMode()]) {  
                    UIView *searchingLabel = PSPDFViewInViewWithPrefix(_self, NSStringFromClass(UILabel.class));  
                    UIView *searchingIndicator = PSPDFViewInViewWithPrefix(_self,  
                                                                            NSStringFromClass(UIActivityIndicatorView.class));  
  
                    if (searchingLabel && searchingIndicator) {  
                        CGRect centeredRect = PSPDFAlignRectangles(searchingLabel.frame, _self.bounds, PSPDFRectAlignCenter);  
                        CGRect searchingLabelRect = searchingLabel.frame;  
                        searchingLabelRect.origin.y = centeredRect.origin.y;  
                        searchingLabel.frame = searchingLabelRect;  
  
                        CGRect indicatorFrame = searchingIndicator.frame;  
                        indicatorFrame.origin.y = searchingLabel.frame.origin.y;  
                        searchingIndicator.frame = indicatorFrame;  
                    }  
                }  
            }  
            @catch (NSEException *exception) {} // noncritical layout issue  
        };  
        PSPDFReplaceMethodWithBlock(printerSearchingViewClass, @selector(layoutSubviews), customLayoutSubviewsSEL,  
                                    customLayoutSubviews);  
    }  
}
```

UITextView & iOS 7



HACKERMONTHLY Issue 39 August 2013

1 of 40





How can we best
encapsulate this fix?

Custom Code in UIViewController

Categories

Subclass

Delegate forwarding

```
@protocol UITextViewDelegate <NSObject, UIScrollViewDelegate>
```

```
@optional
```

```
- (BOOL)textViewShouldBeginEditing:(UITextView *)textView;
```

```
- (BOOL)textViewShouldEndEditing:(UITextView *)textView;
```

```
- (void)textViewDidBeginEditing:(UITextView *)textView;
```

```
- (void)textViewDidEndEditing:(UITextView *)textView;
```

```
- (BOOL)textView:(UITextView *)textView shouldChangeTextInRange:(NSRange)range  
replacementText:(NSString *)text;
```

```
- (void)textViewDidChange:(UITextView *)textView;
```

```
- (void)textViewDidChangeSelection:(UITextView *)textView;
```

```
- (BOOL)textView:(UITextView *)textView shouldInteractWithURL:(NSURL *)URL inRange:  
(NSRange)characterRange NS_AVAILABLE_IOS(7_0);
```

```
- (BOOL)textView:(UITextView *)textView shouldInteractWithTextAttachment:  
(NSTextAttachment *)textAttachment inRange:(NSRange)characterRange  
NS_AVAILABLE_IOS(7_0);
```

```
@end
```

- (BOOL)textView:(UITextView *)textView shouldChangeTextInRange:(NSRange)range replacementText:(NSString *)text;
- (void)textViewDidChange:(UITextView *)textView;
- (void)textViewDidChangeSelection:(UITextView *)textView;

```
UIKIT_EXTERN NSString * const UITextViewTextDidBeginEditingNotification;  
UIKIT_EXTERN NSString * const UITextViewTextDidChangeNotification;  
UIKIT_EXTERN NSString * const UITextViewTextDidEndEditingNotification;
```

- (BOOL)textView:(UITextView *)textView shouldChangeTextInRange:(NSRange)range replacementText:(NSString *)text;
- (void)textViewDidChange:(UITextView *)textView;
- (void)textViewDidChangeSelection:(UITextView *)textView;

```
@interface PSPDFTextView () <UITextViewDelegate>
@property (nonatomic, weak) id<UITextViewDelegate> realDelegate;
@end

- (void)setDelegate:(id<UITextViewDelegate>)delegate {
    if (PSPDFRequiresTextViewWorkarounds()) {
        [super setDelegate:delegate ? self : nil];
        self.realDelegate = delegate != self ? delegate : nil;
    } else {
        [super setDelegate:delegate];
    }
}

- (void)textViewDidChangeSelection:(UITextView *)textView {
    id<UITextViewDelegate> delegate = self.realDelegate;
    if ([delegate respondsToSelector:_cmd]) {
        [delegate textViewDidChangeSelection:textView];
    }

    // Call custom code to fix behavior
}
```

Repetitive Code

```
- (BOOL)textView:(UITextView *)textView shouldInteractWithURL:(NSURL *)URL inRange:
(NSRange)characterRange NS_AVAILABLE_IOS(7_0);

- (BOOL)textView:(UITextView *)textView shouldInteractWithTextAttachment:
(NSTextAttachment *)textAttachment inRange:(NSRange)characterRange
NS_AVAILABLE_IOS(7_0);
```

@end

Message Forwarding

```
- (BOOL)respondsToSelector:(SEL)s {
    return [super respondsToSelector:s] || [self.realDelegate respondsToSelector:s];
}

- (NSMethodSignature *)methodSignatureForSelector:(SEL)s {
    return [super methodSignatureForSelector:s] ?:
        [(id)self.realDelegate methodSignatureForSelector:s];
}

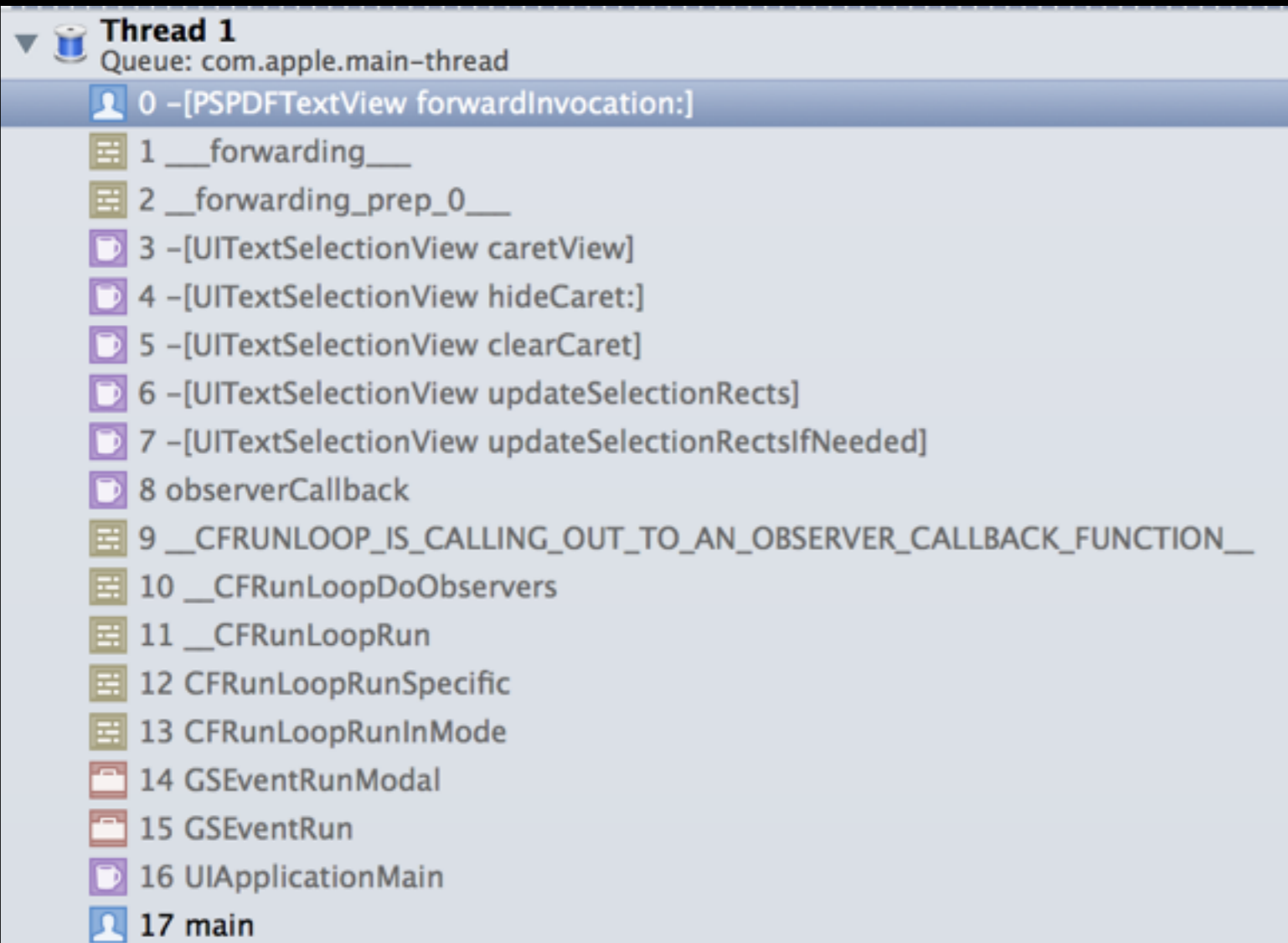
- (void)forwardInvocation:(NSInvocation *)invocation {
    id delegate = self.realDelegate;
    if ([delegate respondsToSelector:invocation.selector]) {
        [invocation invokeWithTarget:delegate];
    }
}
```

Growing Tomatoes

Joe Hewitt

Fasdfasdfa





```
(lldb) po invocation
<NSInvocation: 0xb7efd60>
return value: {@} 0x0
target: {@} 0xec59600
selector: {:} insertionPointColor
```

```
- (UIColor *)insertionPointColor {  
    return UIColor.redColor;  
}  
  
- (void)forwardInvocation:(NSInvocation *)invocation {  
    id delegate = self.realDelegate;  
    if ([delegate respondsToSelector:invocation.selector]) {  
        [invocation invokeWithTarget:delegate];  
    }else {  
        if (invocation.selector == NSSelectorFromString(@"insertionPointColor")) {  
            UIColor *caretColor = CFRetain((__bridge CTypeRef)UIColor.greenColor);  
            [invocation setReturnValue:&caretColor];  
        }  
    }  
}
```

Growing Tomatoes

Joe Hewitt

Edit

Note



I am a green caret



Fasdfasdf



W

E

R

T

Y

U

I

O

P

```
- (void)forwardInvocation:(NSInvocation *)invocation {  
    id delegate = self.realDelegate;  
    if ([delegate respondsToSelector:invocation.selector]) {  
        [invocation invokeWithTarget:delegate];  
    }  
}
```

```
- (void)forwardInvocation:(NSInvocation *)invocation {  
    id delegate = self.realDelegate;  
    if ([delegate respondsToSelector:invocation.selector]) {  
        [invocation invokeWithTarget:delegate];  
    }else {  
        [super forwardInvocation:invocation];  
    }  
}
```

Inspect 3rd party apps
using Reveal

“Web Inspector” for iOS



evasi0n7 - iOS 7.x Jailbreak



Mac OS X

Windows

Compatible with all iPhone, iPod touch, iPad and iPad mini models running iOS 7.0 through 7.0.4



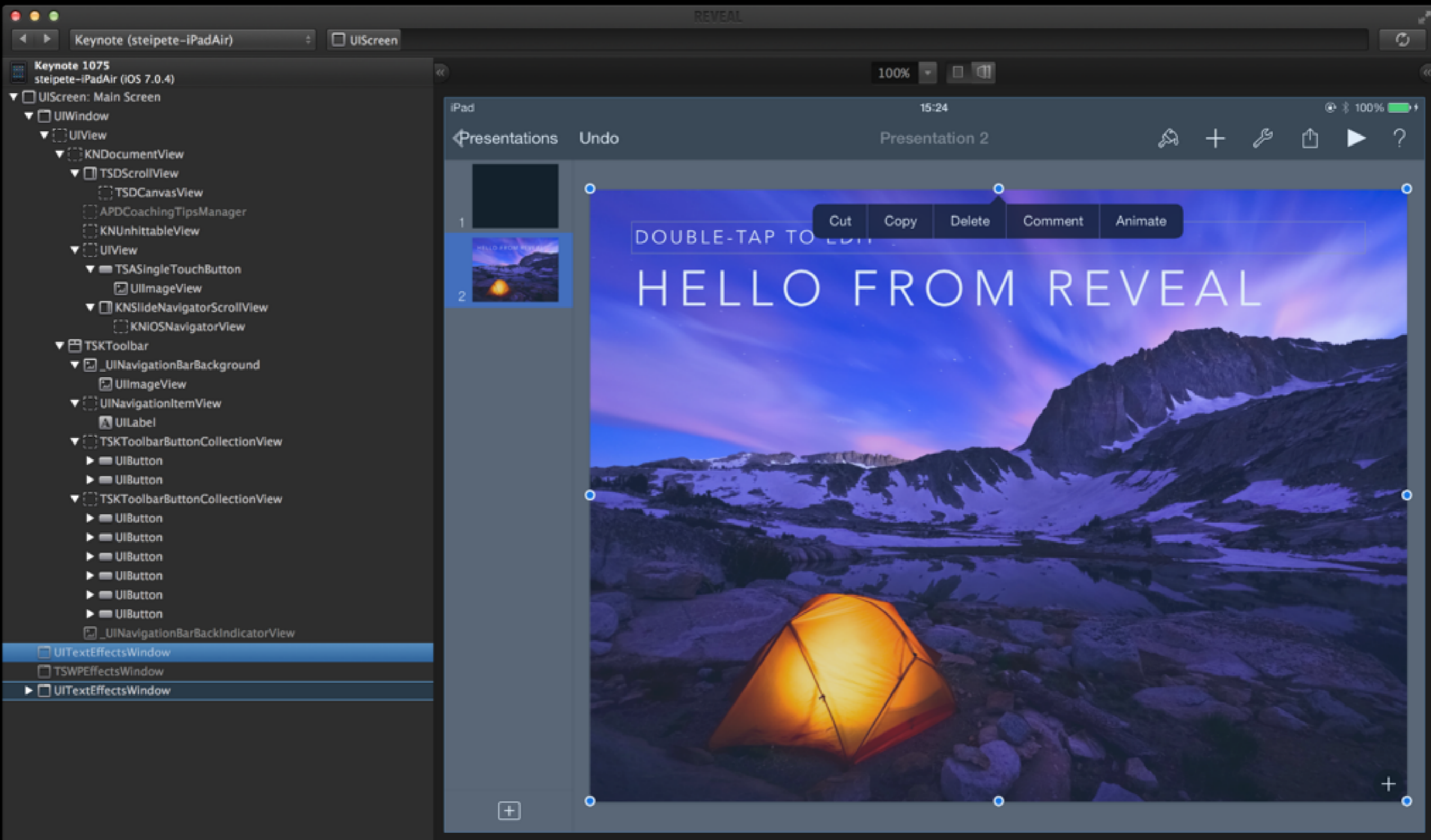
<http://petersteinberger.com/blog/2013/how-to-inspect-the-view-hierarchy-of-3rd-party-apps/>

OpenSSH, CydiaSubstrate

libReveal.dylib

```
scp -r /Applications/Reveal.app/Contents/SharedSupport/iOS-Libraries/  
Reveal.framework root@192.168.0.2:/System/Library/Frameworks
```

```
/Library/MobileSubstrate/DynamicLibraries/libReveal.plist:  
{ Filter = { Bundles = ( "com.Apple.Keynote" ); }; }
```



Keynote (steipete-iPadAir)

UIScreen

Keynote 1075

steipete-iPadAir (iOS 7.0.4)

100%

▼ UIScreen: Main Screen

▼ UIWindow

▼ UIView

▼ KNDocumentView

▼ TSDScrollView

TSDCanvasView

APDCoachingTipsManager

KNUnhittableView

▼ UIView

▼ TSASingleTouchButton

UIImageView

▼ KNSlideNavigatorScrollView

KNiOSNavigatorView

▼ TSKToolbar

▼ _UINavigationControllerBackground

UIImageView

▼ UINavigationControllerItemView

UILabel

▼ TSKToolbarButtonCollectionView

▶ UIButton

▶ UIButton

▼ TSKToolbarButtonCollectionView

▶ UIButton

▶ UIButton

▶ UIButton

▶ UIButton

▶ UIButton

▶ UIButton

▶ UIButton

_UINavigationControllerBackIndicatorView

UITextEffectsWindow

TSWPEffectsWindow

▶ UITextEffectsWindow

iPad

15:2

Presentations

Undo

Present

1

2

DOUBLE-TAP TO EDIT

Cut

Copy

HELLO FROM

We need to go deeper....

lldb

Extract the buildserver

```
hdiutil attach /Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/  
DeviceSupport/7.0.3\ \ (11B508\)/DeveloperDiskImage.dmg
```

```
cp /Volumes/DeveloperDiskImage/usr/bin/debugserver .
```

entitlements.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>com.apple.springboard.debugapplications</key>  
  <true/>  
  <key>run-unsigned-code</key>  
  <true/>  
  <key>get-task-allow</key>  
  <true/>  
  <key>task_for_pid-allow</key>  
  <true/>  
</dict>  
</plist>
```

```
codesign -s - --entitlements entitlements.plist -f debugserver
```

Launch debugserver & connect lldb

Copy signed debugserver to the device

```
./debugserver *:1234 —attach=Keynote
```

lldb

```
platform select remote-ios
```

```
process connect connect://192.168.1.2:1234
```

Launch Debug Server on iPad

```
steipete-iPadAir:~ root# ./debugserver *:1234 --attach=Keynote
debugserver-300.2 for arm64.
Attaching to process Keynote...
Spawning general listening thread.
Spawning kqueue listening thread.
Listening to port 1234 for a connection from *...
Waiting for debugger instructions for process 0.
```

Connect via lldb on Mac

```
steipete@steipete-rmbp ~/Documents/Projects/PSPDFKit/PSPDFKit-Demo $ lldb
(lldb) platform select remote-ios
Platform: remote-ios
Connected: no
SDK Path: "/Users/steipete/Library/Developer/Xcode/iOS DeviceSupport/7.1 (11D5099e)"

(lldb) process connect connect://169.254.101.35:1234
Process 401 stopped
* thread #1: tid = 0x0f23, 0x0000000018eea1cc0 libsystem_kernel.dylib`mach_msg_trap + 8
libsystem_kernel.dylib`mach_msg_overwrite_trap:
    0x18eea1cc4: movn    x16, #31
    0x18eea1cc8: svc     #128
    0x18eea1ccc: ret     lr

(lldb)
```

(lldb)

Print Objects

```
(lldb) po [UIScreen mainScreen]
```

```
<UIScreen: 0x10dc50510; bounds = {{0, 0}, {768, 1024}}; mode =  
<UIScreenMode: 0x10dd01140; size = 1536.000000 x 2048.000000>>
```

```
po [[UIScreen mainScreen] valueForKey:@"scale"]  
2
```

```
p (CGFloat)[[UIScreen mainScreen] scale]  
(CGFloat) $4 = 2
```

Run Expressions

```
expr (void *)[UIApplication sharedApplication] setApplicationIconBadgeNumber:999]
```



Look up Symbols (KVO!)

```
- (void)observeValueForKeyPath:(NSString *)keyPath ofObject:(id)object change:(NSDictionary *)change context:(void *)context {  
    if (context != &PSPDFAnnotationToolbarParentBarAlphaContext) {  
        [super observeValueForKeyPath:keyPath ofObject:object change:change context:context];  
    } else {  
        // custom code...  
    }  
}
```

```
(lldb) image lookup -a `context`
```

```
Address: PSPDFCatalog[0x00000001008823f0] (PSPDFCatalog.__DATA.__bss + 976)
```

```
Summary: PSPDFCatalog`PSPDFAnnotationToolbarParentBarAlphaContext
```

Backtraces

(lldb) bt all

```
* thread #1: tid = 0x74135, 0x00000001001c70f2 PSPDFCatalog`-[PSPDFAnnotationToolbar observeValueForKeyPath:ofObject:change=0x000000010ddcaa80, context=0x00000001008823f0) + 114 at PSPDFAnnotationToolbar.m:725, queue = 'com.apple.main-thread'
  frame #0: 0x00000001001c70f2 PSPDFCatalog`-[PSPDFAnnotationToolbar observeValueForKeyPath:ofObject:change=0x000000010ddcaa80, context=0x00000001008823f0) + 114 at PSPDFAnnotationToolbar.m:725
  frame #1: 0x0000000101dbd982 Foundation`NSKeyValueNotifyObserver + 375
  frame #2: 0x0000000101dbf230 Foundation`NSKeyValueDidChange + 467
  frame #3: 0x0000000101d8224c Foundation`-[NSObject(NSKeyValueObserverNotification) didChangeValueForKey:] + 113
  frame #4: 0x0000000102a306b4 UIKit`-[UINavigationController _positionNavigationBarHidden:edge:] + 113
  frame #5: 0x0000000102a36dc1 UIKit`-[UINavigationController _updateBarsForCurrentInterfaceOrientation:] + 113
  frame #6: 0x0000000102a3cd2f UIKit`-[UINavigationController willAnimateRotationToInterfaceOrientation:duration:] + 113
  frame #7: 0x0000000102a279e4 UIKit`-[UIViewController _willAnimateRotationToInterfaceOrientation:duration:] + 113
  frame #8: 0x0000000102a27deb UIKit`-[UIViewController window:willAnimateRotationToInterfaceOrientation:duration:] + 113
  frame #9: 0x0000000102966b16 UIKit`-[UIWindow _setRotatableClient:toOrientation:updateStatusBar:duration:] + 113
  frame #10: 0x0000000102965a3f UIKit`-[UIWindow _setRotatableClient:toOrientation:updateStatusBar:duration:] + 113
  frame #11: 0x000000010296598f UIKit`-[UIWindow _setRotatableViewOrientation:updateStatusBar:duration:] + 113
  frame #12: 0x0000000102964c9e UIKit`-[UIWindow _updateToInterfaceOrientation:duration:force:] + 377
  frame #13: 0x0000000102964f59 UIKit`-[UIWindow _updateInterfaceOrientationFromDeviceOrientation:] + 377
```

Breakpoints

```
breakpoint set -n PSPDFIsUIKitFlatMode
```

```
breakpoint set -S viewWillAppear:
```

```
breakpoint set -n "-[PSPDFTextSelectionView setSelectedGlyphs:]"
```

```
Breakpoint 9: where = PSPDFCatalog`-[PSPDFTextSelectionView setSelectedGlyphs:] + 52 at  
PSPDFTextSelectionView.m:506, address = 0x0000000100192ea4
```

```
breakpoint list
```

```
breakpoint delete
```

```
po [[UIWindow keyWindow] recursiveDescription]
```

```
<UIWindow: 0x12ed117c0; frame = (0 0; 768 1024); autoresize = W+H; gestureRecognizers = <NSArray: 0x1782466c0>; layer = <UIWindowLayer: 0x17803e2a0>>
(lldb) po [[UIWindow keyWindow] recursiveDescription]
<UIWindow: 0x12ed117c0; frame = (0 0; 768 1024); autoresize = W+H; gestureRecognizers = <NSArray: 0x1782466c0>; layer = <UIWindowLayer: 0x17803e2a0>>
  | <UIView: 0x170168400; frame = (0 0; 768 1024); transform = [0, 1, -1, 0, 0, 0]; autoresize = W+H; gestureRecognizers = <NSArray: 0x17125ac10>;
layer = <CALayer: 0x1700389c0>>
    | <KNDocumentView: 0x1781d4640; frame = (0 0; 1024 768); opaque = NO; autoresize = RM+TM; layer = <CALayer: 0x17823a740>>
    | | <TSDScrollView: 0x12ee7db40; baseClass = UIScrollView; frame = (134 64; 890 704); clipsToBounds = YES; opaque = NO; autoresize = W+H;
autoresizesSubviews = NO; gestureRecognizers = <NSArray: 0x178646cf0>; layer = <CALayer: 0x170a32a40>; contentOffset: {0, 0}>
    | | | <TSDCanvasView: 0x170189e70; frame = (0 0; 890 704); opaque = NO; autoresize = W+H; gestureRecognizers = <NSArray: 0x178641800>;
layer = <TSDCanvasLayer: 0x1702f6180>>
        | <TSDNoDefaultImplicitActionLayer: 0x170a2bd40> (layer)
        | <CALayer: 0x170a31680> (layer)
            | <CALayer: 0x178434160> (layer)
                | <TSDTilingLayer: 0x1782fa380> (layer)
                | <CALayer: 0x178434480> (layer)
                    | <TSDTilingLayer: 0x1782f1a80> (layer)
                    | | <CALayer: 0x1784349c0> (layer)
                    | | <TSDNoDefaultImplicitActionLayer: 0x178434680> (layer)
                    | | <CALayer: 0x1784349e0> (layer)
                        | <TSDTilingLayer: 0x1782f3f80> (layer)
                        | | <CALayer: 0x178434b40> (layer)
                            | <CALayer: 0x178434360> (layer)
                                | <TSDTilingLayer: 0x1782fa480> (layer)
                                | <CALayer: 0x178434460> (layer)
                                    | <TSWPSelectionHighlightLayer: 0x1784343e0> (layer)
                                    | <CAShapeLayer: 0x1784343a0> (layer)
                                    | <TSWPSelectionHighlightLayer: 0x178434340> (layer)
                                    | <TSWPSelectionHighlightLayer: 0x178434120> (layer)
                                | <CALayer: 0x178434b60> (layer)
                                    | <TSDTilingLayer: 0x1782fa700> (layer)
                                    | | <CALayer: 0x178434c00> (layer)
                                        | <CALayer: 0x178434c20> (layer)
                                            | <TSDTilingLayer: 0x1782fa780> (layer)
                                            | <CALayer: 0x178434c40> (layer)
                                                | <TSWPSelectionHighlightLayer: 0x178434c60> (layer)
                                                | <CAShapeLayer: 0x178434c80> (layer)
                                                | <TSWPSelectionHighlightLayer: 0x178434ca0> (layer)
                                                | <TSWPSelectionHighlightLayer: 0x178434cc0> (layer)
                                            | <CAShapeLayer: 0x178434b80> (layer)
                                        | <CALayer: 0x178434be0> (layer)
                                            | <CAShapeLayer: 0x178434b00> (layer)
                                            | <TSWPSelectionHighlightLayer: 0x178434a20> (layer)
                                            | <TSWPSelectionHighlightLayer: 0x178434bc0> (layer)
                                            | <TSWPSelectionHighlightLayer: 0x178434d20> (layer)
                                            | <TSWPSelectionHighlightLayer: 0x178434d40> (layer)
                                | <UIView: 0x17816de00; frame = (0 0; 134 768); autoresize = RM+BM; layer = <CALayer: 0x17823a5a0>>
                                    | <TSASingleTouchButton: 0x12ed4dd80; baseClass = UIButton; frame = (0 724; 134 44); opaque = NO; autoresize = RM+TM; layer =
<CALayer: 0x1782396c0>>
                                        | <UIImageView: 0x12ee84600; frame = (51.5 10.5; 31 23); clipsToBounds = YES; opaque = NO; userInteractionEnabled = NO; layer =
<CALayer: 0x170a35e20>>
                                            | <KNSlideNavigatorScrollView: 0x12ee7faa0; baseClass = UIScrollView; frame = (0 64; 134 660); clipsToBounds = YES; opaque = NO;
autoresize = W+H; gestureRecognizers = <NSArray: 0x178642f70>; layer = <CALayer: 0x170a2ab80>; contentOffset: {0, 0}>
                                            | <KNiOSNavigatorView: 0x12ee7ffe0; frame = (0 0; 134 660); opaque = NO; autoresize = W+H; layer = <KNNavigatorLayer:
0x12ee803a0>>
                                                | <KNiOSiPadSlideNavigatorSlideLayer: 0x17016e280> (layer)
```

Keynote (steipete-iPadAir)

UIScreen

Keynote 1075

steipete-iPadAir (iOS 7.0.4)

100%

▼ UIScreen: Main Screen

▼ UIWindow

▼ UIView

▼ KNDocumentView

▼ TSDScrollView

TSDCanvasView

APDCoachingTipsManager

KNUnhittableView

▼ UIView

▼ TSASingleTouchButton

UIImageView

▼ KNSlideNavigatorScrollView

KNiOSNavigatorView

▼ TSKToolbar

▼ _UINavigationControllerBackground

UIImageView

▼ UINavigationControllerItemView

UILabel

▼ TSKToolbarButtonCollectionView

▶ UIButton

▶ UIButton

▼ TSKToolbarButtonCollectionView

▶ UIButton

▶ UIButton

▶ UIButton

▶ UIButton

▶ UIButton

▶ UIButton

_UINavigationControllerBackIndicatorView

UITextEffectsWindow

TSWPEffectsWindow

▶ UITextEffectsWindow

iPad

15:2

Presentations

Undo

Present

1

2

Cut

Copy

DOUBLE-TAP TO EDIT

HELLO FROM

```
| | | | <TSDCanvasView: 0x170189e70; frame = (0 0; 890 704); opaque = NO; autoresize = W+H; gestureRecognizers =  
<NSArray: 0x178641800>; layer = <TSDCanvasLayer: 0x1702f6180>>  
| | | | | <TSDNoDefaultImplicitActionLayer: 0x170a2bd40> (layer)  
| | | | | <CALayer: 0x170a31680> (layer)  
| | | | | | <CALayer: 0x178434160> (layer)  
| | | | | | | <TSDTilingLayer: 0x1782fa380> (layer)  
| | | | | | | <CALayer: 0x178434480> (layer)  
| | | | | | | | <TSDTilingLayer: 0x1782f1a80> (layer)  
| | | | | | | | | <CALayer: 0x1784349c0> (layer)  
| | | | | | | | | <TSDNoDefaultImplicitActionLayer: 0x178434680> (layer)  
| | | | | | | | | <CALayer: 0x1784349e0> (layer)  
| | | | | | | | | <TSDTilingLayer: 0x1782f3f80> (layer)  
| | | | | | | | | | <CALayer: 0x178434b40> (layer)  
| | | | | | | | | | | <CALayer: 0x178434360> (layer)  
| | | | | | | | | | | | <TSDTilingLayer: 0x1782fa480> (layer)  
| | | | | | | | | | | | <CALayer: 0x178434460> (layer)  
| | | | | | | | | | | | <TSWPSelectionHighlightLayer: 0x1784343e0> (layer)  
| | | | | | | | | | | | <CAShapeLayer: 0x1784343a0> (layer)  
| | | | | | | | | | | | <TSWPSelectionHighlightLayer: 0x178434340> (layer)  
| | | | | | | | | | | | <TSWPSelectionHighlightLayer: 0x178434120> (layer)  
| | | | | | | | | | <CALayer: 0x178434b60> (layer)  
| | | | | | | | | | | <TSDTilingLayer: 0x1782fa700> (layer)  
| | | | | | | | | | | <CALayer: 0x178434c00> (layer)  
| | | | | | | | | | | | <CALayer: 0x178434c20> (layer)  
| | | | | | | | | | | | | <TSDTilingLayer: 0x1782fa780> (layer)  
| | | | | | | | | | | | | <CALayer: 0x178434c40> (layer)  
| | | | | | | | | | | | | <TSWPSelectionHighlightLayer: 0x178434c60> (layer)  
| | | | | | | | | | | | | <CAShapeLayer: 0x178434c80> (layer)  
| | | | | | | | | | | | | <TSWPSelectionHighlightLayer: 0x178434ca0> (layer)  
| | | | | | | | | | | | | <TSWPSelectionHighlightLayer: 0x178434cc0> (layer)  
| | | | | | | | | | | <CAShapeLayer: 0x178434b80> (layer)  
| | | | | | | | | | <CALayer: 0x178434be0> (layer)  
| | | | | | | | | | | <CAShapeLayer: 0x178434b00> (layer)  
| | | | | | | | | | | <TSWPSelectionHighlightLayer: 0x178434a20> (layer)  
| | | | | | | | | | | <TSWPSelectionHighlightLayer: 0x178434bc0> (layer)  
| | | | | | | | | | | <TSWPSelectionHighlightLayer: 0x178434d20> (layer)  
| | | | | | | | | | | <TSWPSelectionHighlightLayer: 0x178434d40> (layer)  
| | | | | <UIView: 0x17816de00; frame = (0 0; 134 768); autoresize = RM+BM; layer = <CALayer: 0x17823a5a0>>  
| | | | | <TSASingleTouchButton: 0x12ed4dd80; baseClass = UIButton; frame = (0 724; 134 44); opaque = NO; autoresize =  
RM+TM; layer = <CALayer: 0x1782396c0>>  
| | | | | <UIImageView: 0x12ee84600; frame = (51.5 10.5; 31 23); clipsToBounds = YES; opaque = NO;  
userInteractionEnabled = NO; layer = <CALayer: 0x170a35e20>>  
| | | | | <KNSlideNavigatorScrollView: 0x12ee7faa0; baseClass = UIScrollView; frame = (0 64; 134 660); clipsToBounds =
```

```
(lldb) po [[[[[[[[UIWindow keyWindow] rootViewController] view] subviews] firstObject] subviews] firstObject] subviews] firstObject]
```

```
<TSDCanvasView: 0x170189e70; frame = (0 0; 890 704); opaque = NO; autoresize = W+H; gestureRecognizers = <NSArray: 0x178641800>; layer = <TSDCanvasLayer: 0x1702f6180>>
```

```
(lldb) p (char *)ivar_getName(((struct objc_ivar **)class_copyIvarList([TSDCanvasView class], NULL))[0])
```

```
(char *) $17 = 0x000000010186577c "mController"
```

```
(lldb) p (char *)ivar_getName(((struct objc_ivar **)class_copyIvarList([TSDCanvasView class], NULL))[1])
```

```
(char *) $18 = 0x0000000101866225 "mLayerHost"
```

```
(lldb) po [[[[[[[[[UIWindow keyWindow] rootViewController] view] subviews] firstObject] subviews]  
firstObject] subviews] firstObject] valueForKey:@"mController"]
```

```
<KNInteractiveCanvasController: 0x137e6e800>
```

Cycript

```
cy# UIApp
"<SpringBoard: 0x266f00>"
```

```
cy# UIApp->_uiController.window
"<SBAppWindow: 0x27ac10; baseClass = UIWindow; frame = (0 0; 320 480); layer = <CALayer: 0x27aba0>>"
```

```
cy# UIApp->_uiController.window.subviews[0].subviews
["<UIImageView: 0x4b3cea0; frame = (0 0; 320 480); opaque = NO; userInteractionEnabled = NO; layer = <CALayer: 0x4a75550>>", "<UIView: 0x4b4ba80; frame = (0 0; 320 480); autoresize = W+H; layer = <CALayer: 0x4b4bbf0>>"]
```

```
cy# UIApp->_uiController.window.subviews[0].subviews[1].subviews
["<SBIconContentView: 0x4b4bc20; frame = (0 40; 320 349); autoresize = H; layer = <CALayer: 0x4a613c0>>", "<UIView: 0x4a25250; frame = (0 389; 320 91); layer = <CALayer: 0x4a38630>>"]
```

```
cy# UIApp->_uiController.window.subviews[0].subviews[1].subviews[0].subviews
["<SBIconListPageControl: 0x27aab0; baseClass = UIPageControl; frame = (0 330; 320 19); autoresize = TM; layer = <CALayer: 0x4b3c370>>", "<SBIconScrollView: 0x4a62360; baseClass = UIScrollView; frame = (0 0; 320 330); autoresize = H; layer = <CALayer: 0x4a624e0>>"]
```

```
cy# var pages = UIApp->_uiController.window.subviews[0].subviews[1].subviews[0].subviews[0]
```

```
cy# pages.currentPage
```

```
1
```

```
cy# pages.numberOfPages
```

```
15
```

Inject Code (again)

Building a .dylib

```
export SYSROOT=/Applications/Xcode.app/Contents/Developer/Platforms/  
iPhoneOS.platform/Developer/SDKs/iPhoneOS7.0.sdk/
```

```
clang -dynamiclib -isysroot ${SYSROOT} -arch arm64  
-framework Foundation -o debughelper.dylib debughelper.m
```



debughelper.m



debughelper.dylib

debughelper.m

```
Class class = [self class];
u_int count;
Ivar *ivars = class_copyIvarList(class, &count);
NSMutableDictionary *ivarDictionary = [NSMutableDictionary dictionary];
for (int i = 0; i < count ; i++) {
    NSString *ivarStr = @(ivar_getName(ivars[i]));
    NSString *typeEncoding = @(ivar_getTypeEncoding(ivars[i]));
    id obj = [self valueForKey:ivarStr];
    [ivarDictionary setObject:obj ?: NSNull.null forKey:ivarStr];
}
free(ivars);
```



169.254.101.35



View



Window



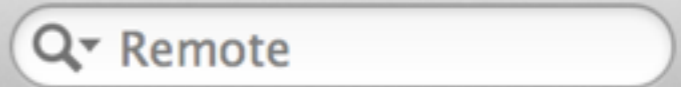
Quick Look



Action



Sync



Search



Library

MobileSubstrate



DynamicLibraries



Name ▲

Size

Date



debughelper.dylib

38 KB

10 Jan 2014 20:22



debughelper.plist

53 B

10 Jan 2014 16:34



libReveal.dylib

3,9 MB

10 Jan 2014 11:42



libReveal.plist

53 B

10 Jan 2014 13:30



MobileSafety.dylib

24 KB

04 Feb 2013 05:44



MobileSafety.plist

118 B

04 Feb 2013 05:44



lldb: image list

[208] 8B556756-7ABC-3187-AFBB-5ACF49DF16E1 0x00000000102ac0000 /Library/
MobileSubstrate/DynamicLibraries/libReveal.dylib (0x00000000102ac0000)

[207] 3D135F89-88B8-33FC-8698-724BFB44F6A2 0x00000000102ab4000 /Library/
MobileSubstrate/DynamicLibraries/debughelper.dylib (0x00000000102ab4000)

```
(lldb) po [[[[[[[[[[UIWindow keyWindow] rootViewController] view] subviews] firstObject]
subviews] firstObject] subviews] firstObject] valueForKey:@"mController"] classInfo]
{
    ivars =      (
        "mShow : @\"KNShow\\\"\",
        "mSlideNode : @\"KNSlideNode\\\"\",
        "mSlide : @\"KNAbstractSlide\\\"\",
        "mUIControlsViewController : @\"KNUIControlsViewController\\\"\",
        "mOriginalY : d\",
        "mTopRulerView : @\"KNRulerView\\\"\",
        "mSideRulerView : @\"KNRulerView\\\"\",
        "mRulerMiddleView : @\"UIView\\\"\",
        "mUnhiddenInfos : @\"NSArray\\\"\",
        "mRulersVisible : B\",
        "mStoppedUIIdleTimer : B\",
        "mEditingAnimations : B\",
        "mIsSuppressingInterfaceGestures : B\",
        "mSuppressZoomOnSelectionChange : B\",
        "mForceSuppressSpellChecking : B\",
        "mDisplayRulerAfterKeyboardHidden : B\",
        "mFadesDrawablesOutsideSlide : B\",
        "mDrawableFadeMaskSublayers : @\"NSArray\\\"\",
        "mDrawableFadeMaskLayer : @\"CALayer\\\"\",
        "mBackgroundDecorators : @\"NSMutableArray\\\"\",
        "mSlideShadowLayer : @\"CALayer\\\"\",
        "mSlideHidden : B\",
        "mActionGhostManager : @\"KNActionGhostManager\\\"\",
        "mRepDragTrackerDelegate : @\"KNRepDragTrackerDelegate\\\"\",
        "mHyperlinkDelegate : @\"NSObject<KNHyperlinkDelegate>\\\"\",
        "mChunksToSelectWhenAutomaticCommandGroupCloses : @\"NSMutableSet\\\"\",
        "mSlideShadowColor : @\"TSUColor\\\"\",
```

```
(lldb) po [[[UIWindow keyWindow] rootViewController] childViewControllers] objectAtIndex:1]
<TSADocumentManagerViewController: 0x15004e200>
```

```
(lldb) po [[[[[UIWindow keyWindow] rootViewController] childViewControllers] objectAtIndex:1] dump]
{
```

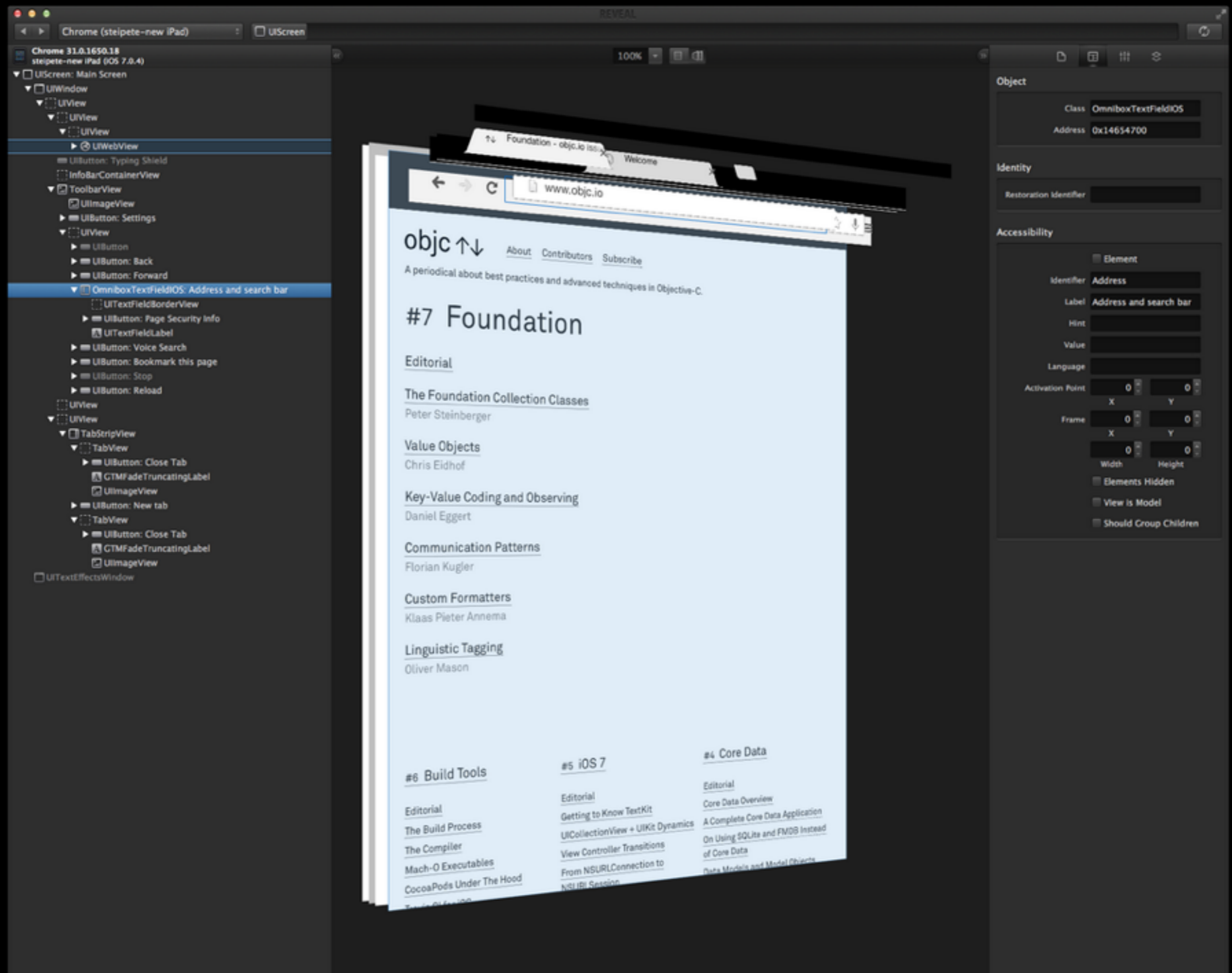
```
    ivars = {
        "_addActionViewController_@"TIADocumentManagerActionViewController\"" = "<null>";
        "_addButton_@"UIBarButtonItem\"" = "<UIBarButtonItem: 0x1781ab280>";
        "_cacheInReverseOrder_B" = 0;
        "_coachingTipsButton_@"UIBarButtonItem\"" = "<UIBarButtonItem: 0x1781ab6e0>";
        "_conflictResolutionAnimator_@"TSAConflictResolutionAnimator\"" = "<null>";
        "_currentInvictionDocumentPath_@"NSString\"" = "<null>";
        "_currentSyncFileCoordinator_@"NSFileCoordinator\"" = "<null>";
        "_debugSyncPopoverController_@"TSASyncDebugPopoverController\"" = "<null>";
        "_delegate_@"<TSADocumentManagerDelegate>\"" = "<KNDocumentManagerDelegate: 0x1780143c0>";
        "_deleteButton_@"UIBarButtonItem\"" = "<null>";
        "_didSendCopyManagerAppear_B" = 0;
        "_disableInterfaceOrientationCount_Q" = 0;
        "_dismissProgressViewCompletionBlock_@" = "<null>";
        "_documentCollection_@"TIADocumentCollection\"" = "<TIADocumentCollection: 0x17828ba40>\n\t<infos>\n\t\t(\n\t\t\t<TIADocumentManagerMetaItemInfo: 0x17801af10>\",\n\t\t\t\"(TIADocumentInfo*)0x1781a8dc0; filename=Presentation 2.key;\n\t\t\tfolder=(null); date=2014-01-10 17:36:10 +0000 synced=NO materialized=YES\", \n\t\t\t\"(TIADocumentInfo*)0x1701a9680;\n\t\t\tfilename=Presentation.key; folder=(null); date=2014-01-10 14:21:34 +0000 synced=NO materialized=YES\"\\n)\n\t\t\t</infos>\n\t\t\t<currentlyOpenDocumentInfo>\n\t\t\t\t(null)\n\t\t\t</currentlyOpenDocumentInfo>\n\t\t\t</TIADocumentCollection>";
        "_dragOriginFolderInfo_@"TIAFolderInfo\"" = "<null>";
        "_duplicateButton_@"UIBarButtonItem\"" = "<null>";
        "_editButton_@"UIBarButtonItem\"" = "<UIBarButtonItem: 0x1781ab600>";
        "_editFolderNameAfterExpandAnimation_B" = 0;
        "_expandedFolderInfo_@"TIAFolderInfo\"" = "<null>";
        "_folderView_@"TSADocumentManagerFolderView\"" = "<null>";
        "_gridHeaderView_@"TSADocumentManagerHeaderView\"" = "<TSADocumentManagerHeaderView: 0x178196650; frame = (0 0; 1024 58); layer = <CALayer: 0x178628380>>";
        "_gridViewConfiguration_@"TSADocumentManagerViewConfiguration\"" = "<TSADocumentManagerViewConfiguration: 0x1780f8a80>";
        "_gridView_@"TSADocumentManagerView\"" = "<TSADocumentManagerView: 0x1500c3800; baseClass = UIScrollView; frame = (0 0; 1024 704); autoresize = W+H; autoresizingSubviews = NO; gestureRecognizers = <NSArray: 0x178e4f300>; layer = <CALayer: 0x178627f40>; contentOffset: {0, 58}>";
        "_hasAlreadyAppeared_B" = 1;
        "_iCloudShareSettingsViewController_@"TIAiCloudShareSettingsViewController\"" = "<null>";
        "_importAnimator_@"TSAImportAnimator\"" = "<null>";
        "_importedDocumentInfo_@"TIADocumentInfo\"" = "<null>";
        "_isCancelingDownloadAndOpen_B" = 0;
        "_isOpeningOrImportingInPlace_B" = 0;
```

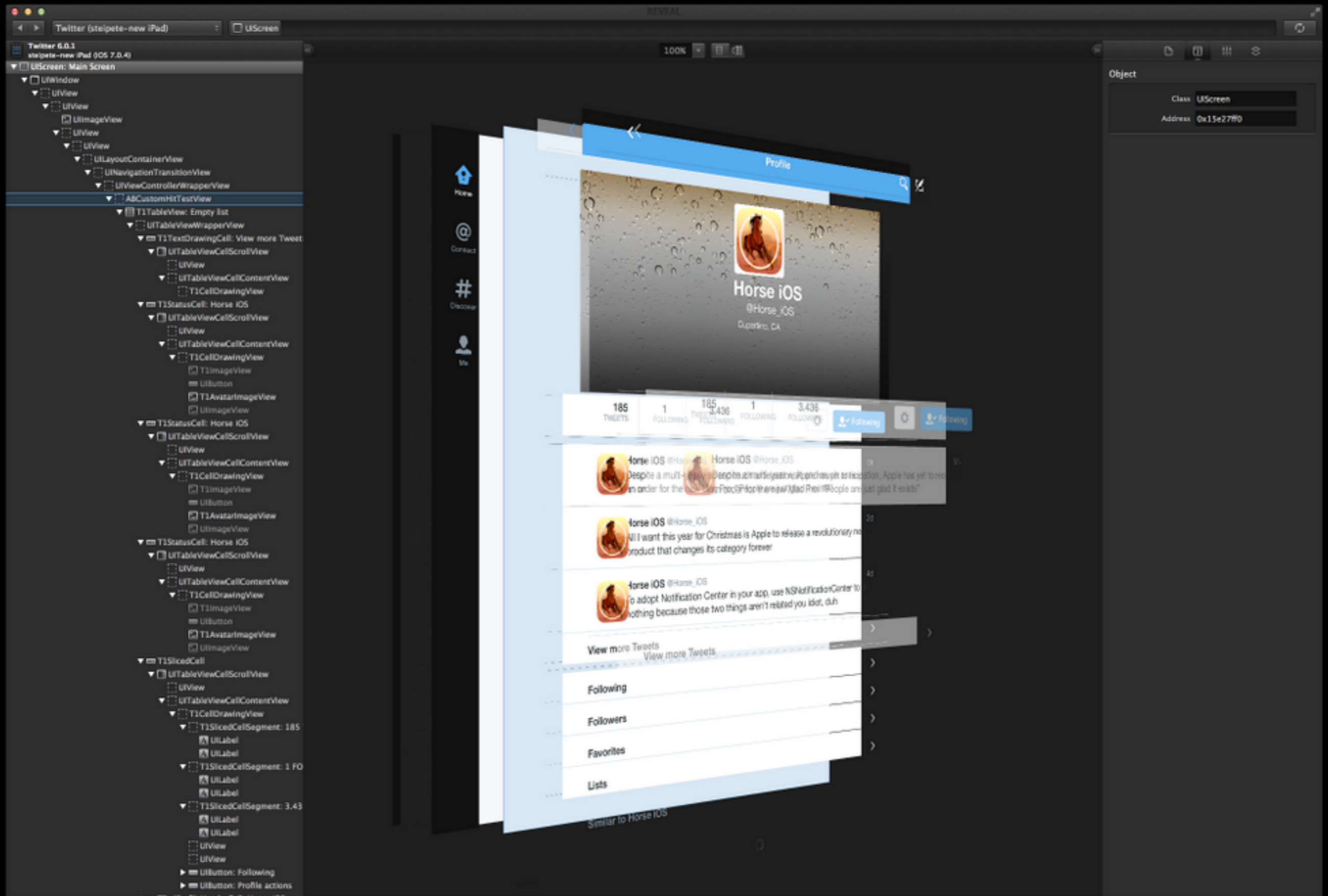
New in iOS 7

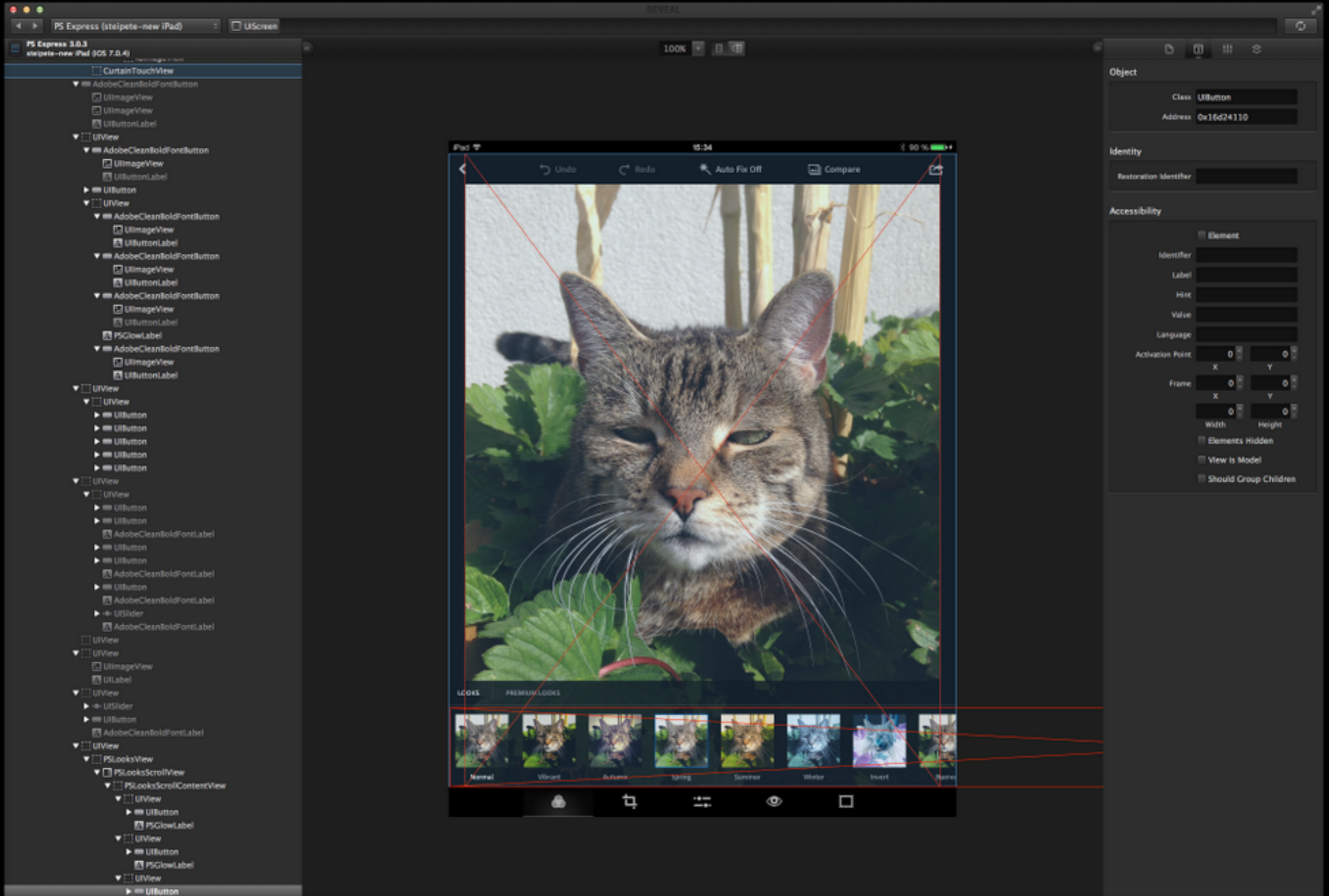
_ivarDescription

_methodDescription

_shortMethodDescription







Thanks!

Peter Steinberger
@steipete

<http://petersteinberger.com/blog/2013/how-to-inspect-the-view-hierarchy-of-3rd-party-apps/>