

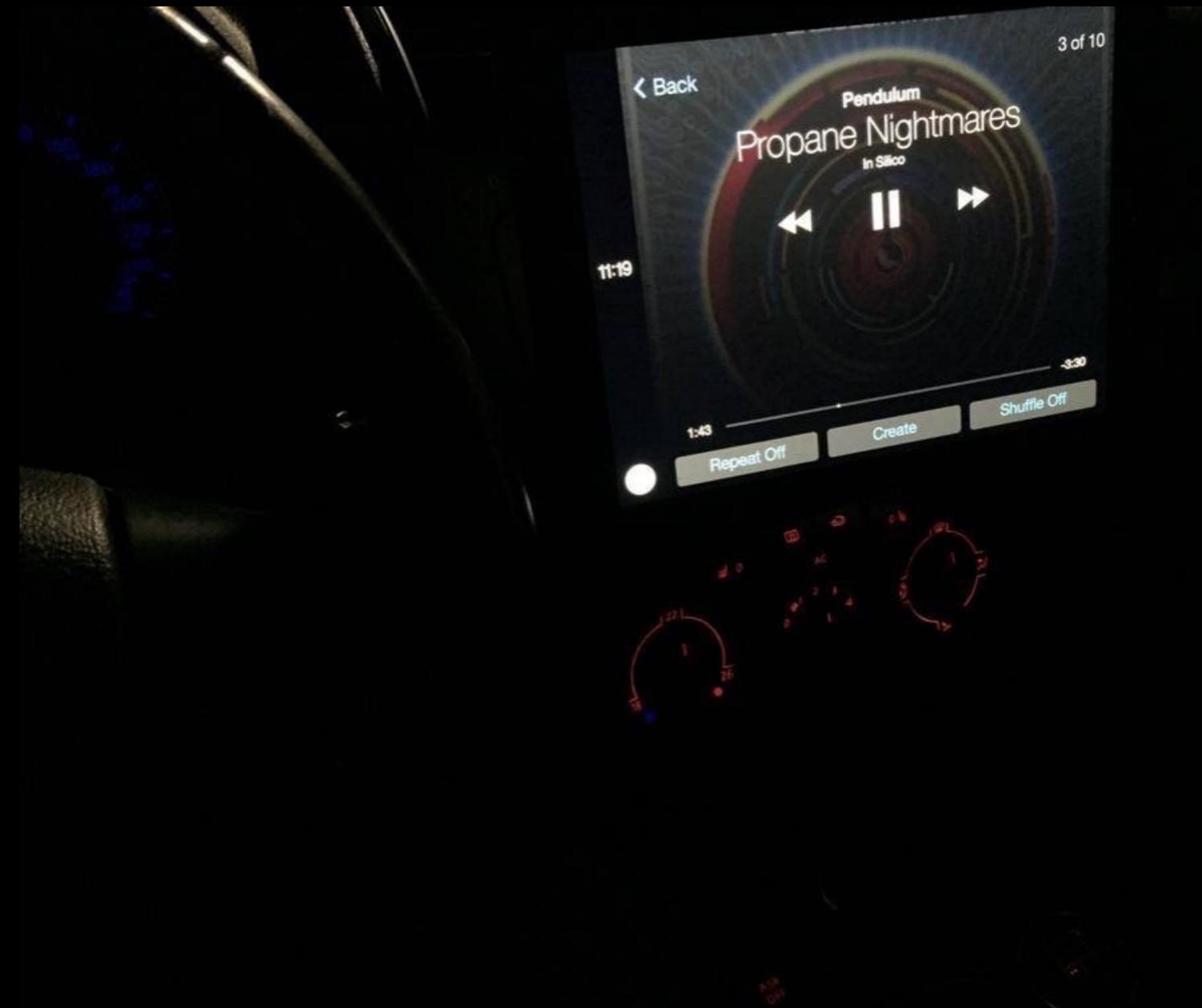
GETTING AHEAD OF THE CURVE

ADAM BELL | NSSPAIN 2015

BIT OF HISTORY



Chat Heads
hack for iOS



Ignition (CarPlay on iPad hack)

BIT OF HISTORY

REDACTED



Native UIKit Apps on  WATCH

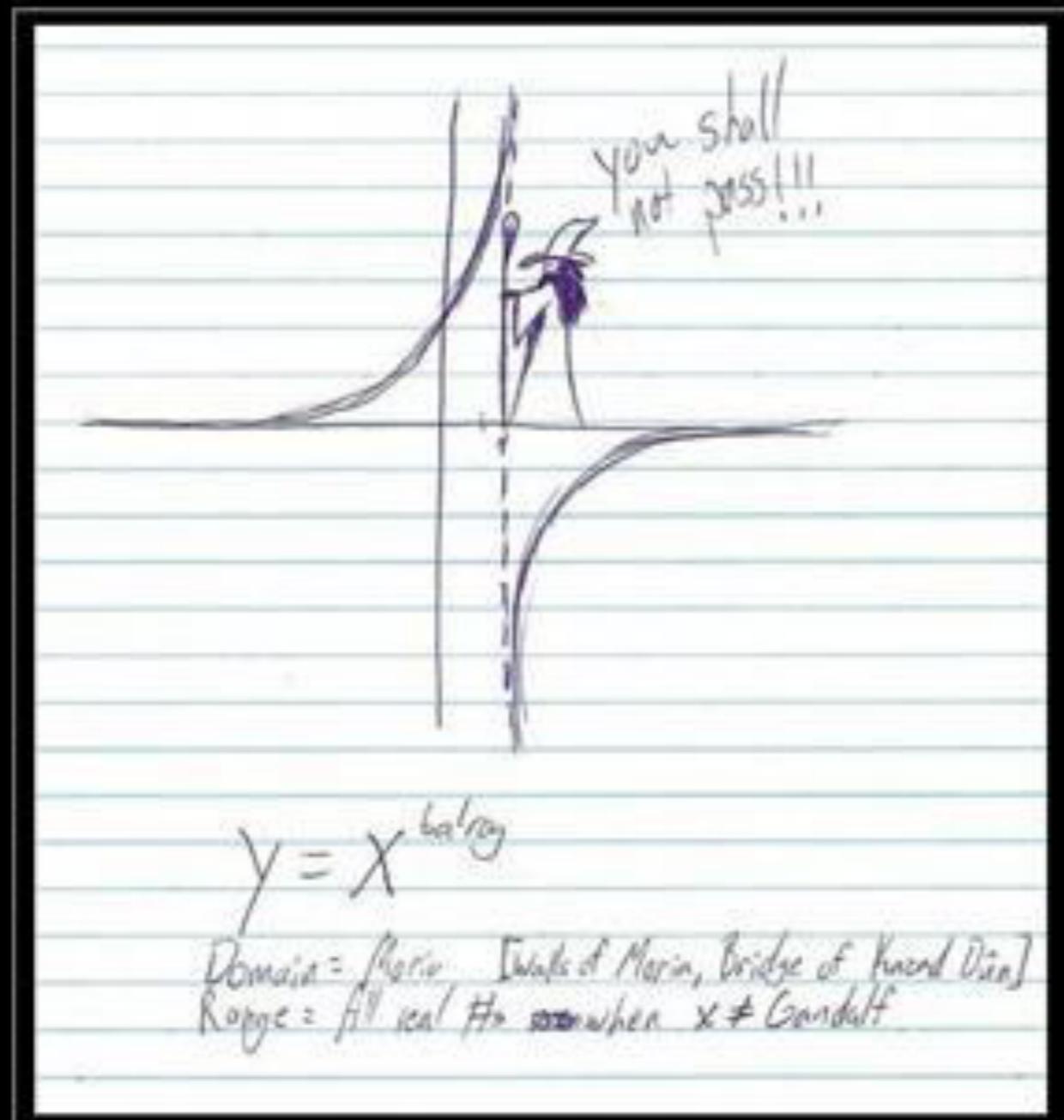
LET'S TALK CURVES...

LOTS OF TYPES OF CURVES



MATHEMATICAL CURVES

$$y = -1/x$$



LITERAL CURVE TYPE

- [UIBezierPath
bezierPathWithArcCenter:CGPointMake(0,0)
radius:9001
startAngle:M_PI
endAngle:(M_PI / 2.0)
clockwise:**SURE**];
- BOOL a == (YES ? NO ? SURE);
- type... geddit?

THINK OUTSIDE THE... CURVE

- "Siri, what's getting ahead of the curve?"
- "I dunno, but I found these web results for you:"
 - 
- **ahead of the curve**: ahead of current thinking or trends.

EXAMPLES

- loops, à la Sonic the Hedgehog
 - gotta go fast
- Apple is ahead of the curve. Samsung is not.
- AutoLayout™ is... nope, not even gonna go there.
- :)



PICTURE EXAMPLE

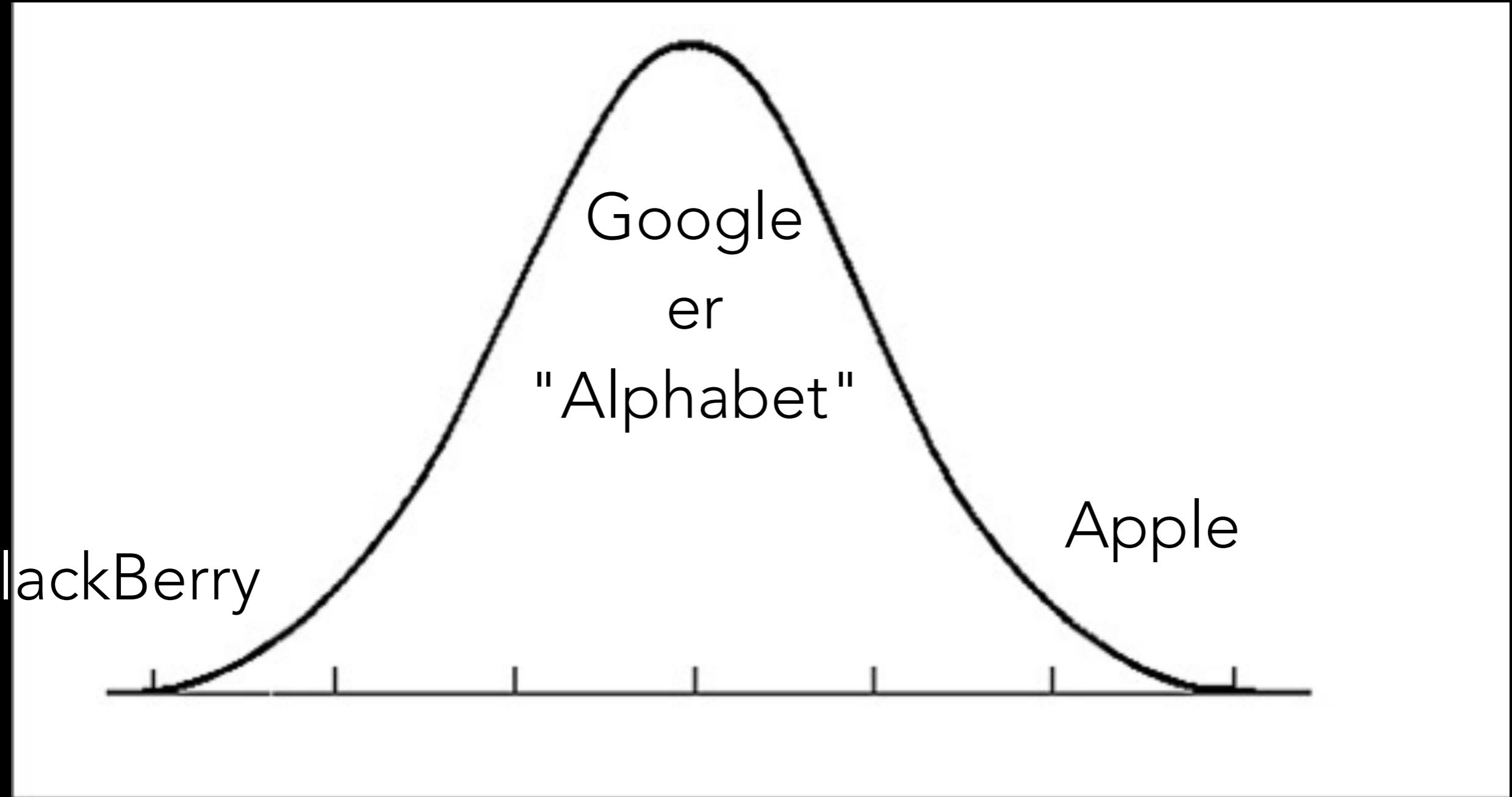
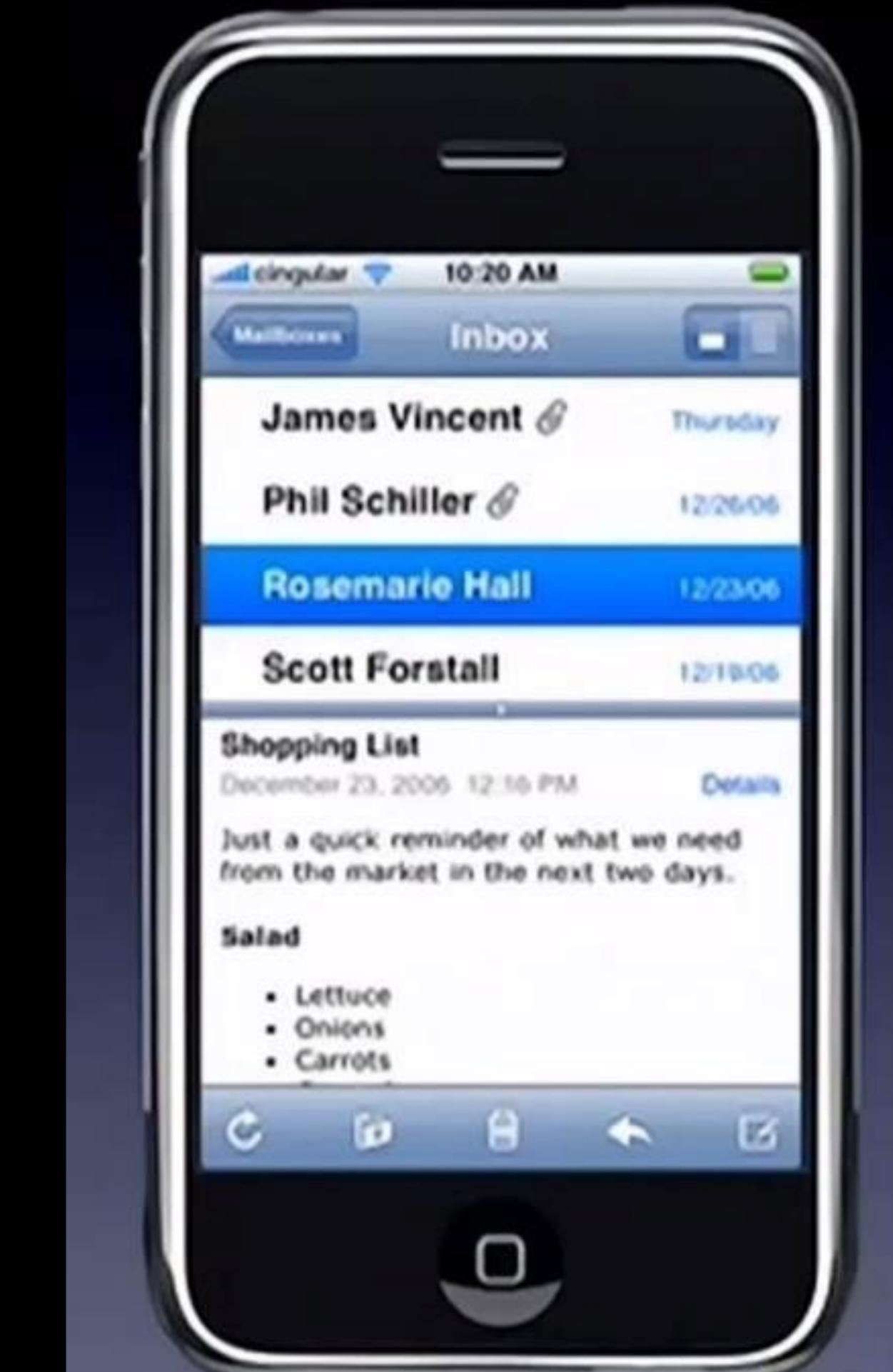


photo cred: @NeoNacho

ADVANCED PROTOTYPES

- since the dawn of time, Apple's been pushing the boundaries of design and what's expected.
- they do this with crazy cool prototypes!
- why can't we do that too?



WWDC

Keynote icon in keynote is super meta

- at WWDC Apple had an "advanced prototyping" session
 - aka how to use Magic Move in Keynote :P
 - coined the term "Fake it, till you make it"
 - why not just make it?

super meta



LOTS OF WAYS TO PROTOTYPE!



Form



Quartz Composer



Origami

Apparently every prototyping tool ever
needs a blue icon?

↖(ツ)↗

ON WORKING WITH DESIGNERS...

- never say no to a prototype or design
- "that's not physically possible."
 - no u
 - hard != impossible
 - if it's actually impossible, make it less impossible

HOWEVER...

if it's android...

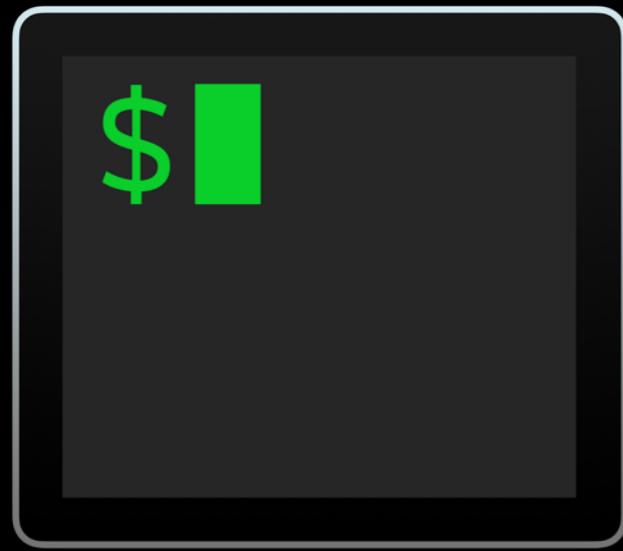
it's already impossible.

:)

PERSONALLY I PREFER...
XCODE + HAX



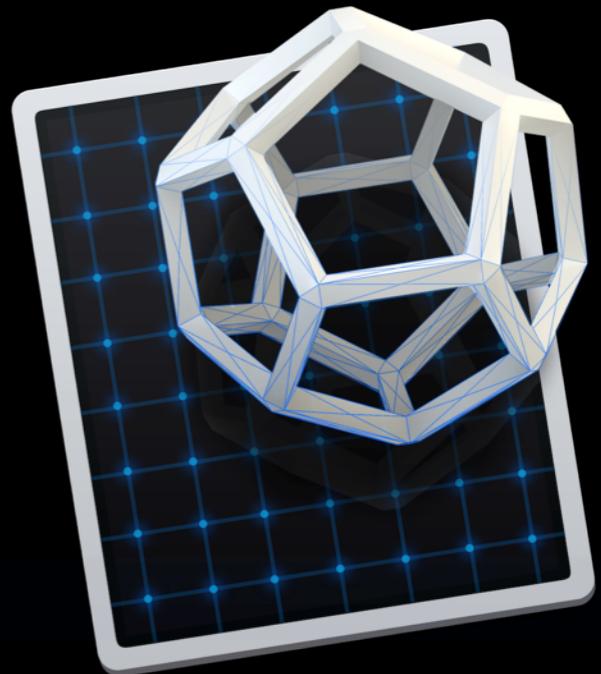
SOME TRICKS OF THE TRADE



class-dump



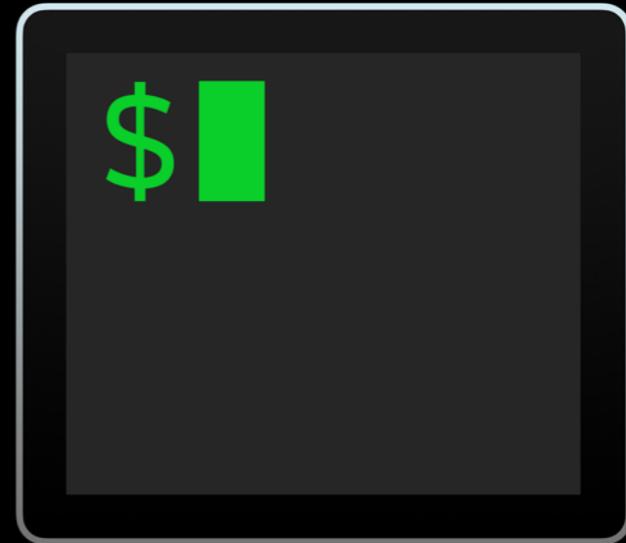
atom/sublime/w.e



hopper

CLASS-DUMP

- well... it dumps classes.
 - as headers
 - excellent for surveying the (private) API landscape
 - works awesome with Atom / Sublime
 - searching headers with quick open!



HOPPER DISASSEMBLER

- my personal favourite
- disassembles binaries
 - spits out assembly or half-baked C code.
 - yay assembly! :D



REAL LIFE SITUATION

APPLE KEYNOTE DEV CYCLE

0. New device / feature

1. OMG

2. Adapt new API

4. YOLO, SHIP IT



TIM COOK HOLDING THINGS

All the money from an earnings call



TIM COOK HOLDING THINGS

Rose Gold iPhone 6S+



TIM COOK HOLDING THINGS

Tim Cook



BASICALLY....
TIM COOK HOLDING THINGS...

SHOULD BE A MEME.

#TIMCOOKHOLDINGTHINGS

#NSSPAIN15



APPLE KEYNOTE DEV CYCLE

0. New device / feature

1. OMG

2. Adapt new API

4. YOLO, SHIP IT



WAIT, WHAT ABOUT 3.?

APPLE KEYNOTE DEV CYCLE

- we ship apps for new devices... without testing
 - just to be ready for day 1
 - remember watchOS 1?
 - this is insanity
 - we can do better



MAKE FEATURES BEFORE THEY EXIST



AKA

MAKE SOMETHING COOL...

BEFORE SOMEONE ELSE DOES



MAKE FEATURES BEFORE THEY EXIST

- anticipate newer features
 - prototype possible things
- play with upcoming ones
 - if you don't haz, mimic them
 - if you can't mimic, fake them
- tl;dr: get a feel for how they work

HOW?

- Private API
- Private API
- Private API
 - seriously. 3D touch was leaked like 2 betas early.
 - 2 weeks to dev → 2 months

3D TOUCH LEAK

 Hamza Sood
@hamzasood

Following

Some force touch code in iOS. Looks like they've tested kb trackpad gestures on the 6s, activated via force touch

```
Pseudo Code
 Remove potentially dead code
 Remove LO/HI macros
void * -[_UITextSelectionSettings enableDeepPress](void * self, void * _cmd) {
    rax = self->_enableDeepPress;
    return rax;
}
```

RETWEETS FAVORITES

154 131



6:37 PM - 26 Aug 2015



PRIVATE API

- stuff Apple doesn't want you to see / use
 - don't use it publicly.
 - unless you're a ninja.
- usually prefixed with **underscores**
 - -__DO_NOT_USE_OR_YOU_WILL_BE_FIRED:
 - ^ cool method name

PRIVATE API

- unreleased features! :D
 - excellent for prototyping new / experimental things
 - basically the entire jailbreak community prides itself on messing with internal Apple things :)
 - free things are free!

PRIVATE API

- don't ship it. ever.
- apple can change it at anytime
 - which could lead to app instability
 - which makes your users :(
- k?
- k sweet.

THIS ONE COOL TRICK...

- how 2 b a cool prototyping person
- use what you have to fake something you don't
 - ... doesn't matter if it's good
 - just do it

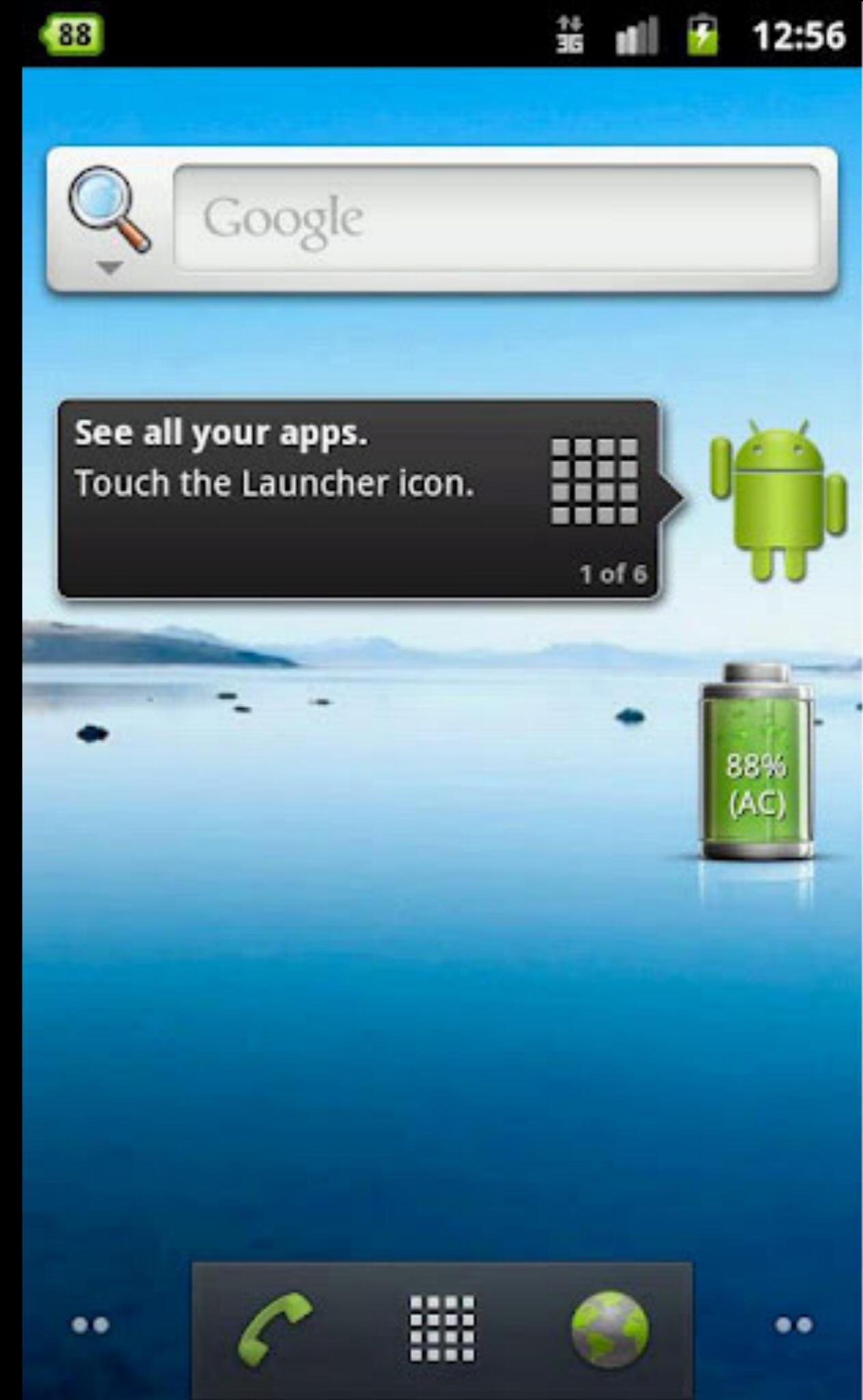


FUNNY PRIVATE API

- internalUpdateConstraintsIfNeededAccumulatingViews
 NeedingSecondPassAndViewsNeedingBaselineUpdate
 - that's a mouthful^
- __Multithreading_Violation_AllThatIsLeftToUsIsHonor__
- - [AVPlayerLayer playerLayerWithPlayer:]

WIDGETS

sup?



WIDGETS

- convenient access to simple information
- android already has 'em (yay?)
- we'd all love them on SpringBoard
 - not notification center
 - Apple hasn't given us access yet, maybe someday!
 - jk let's make them anyways...

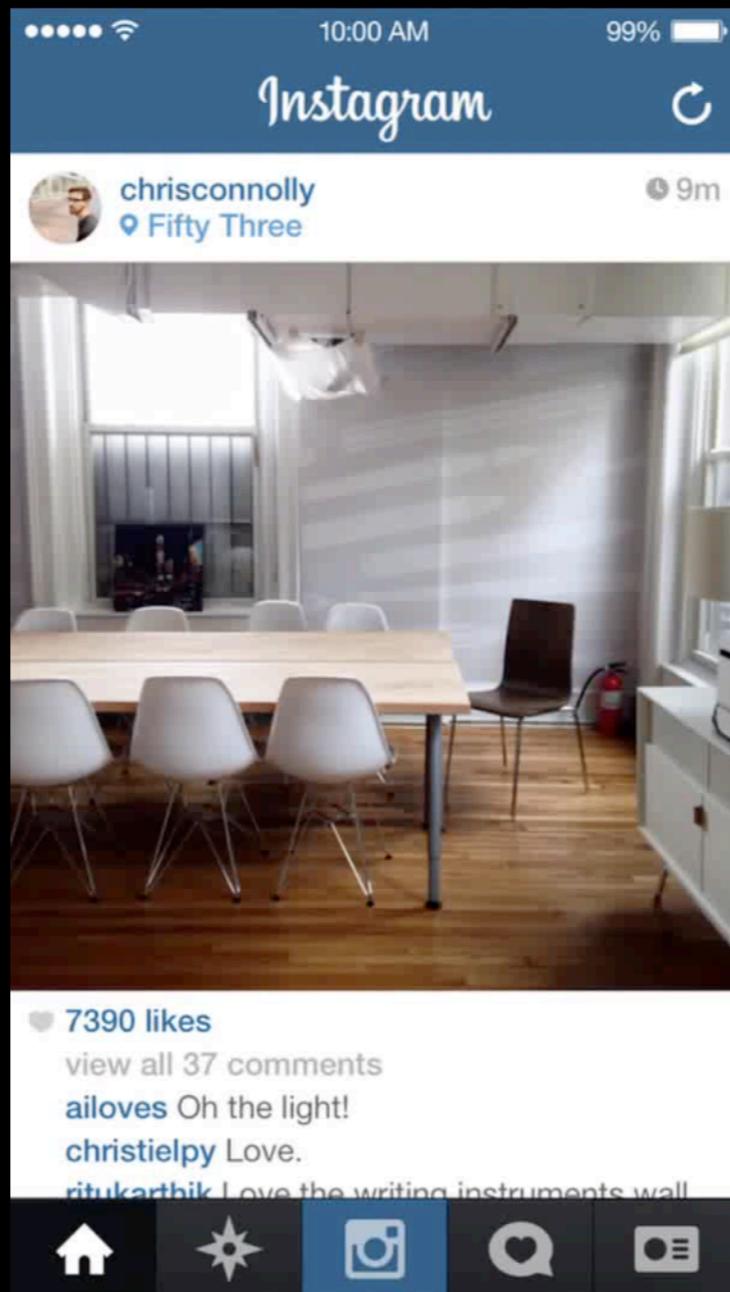


DOOM'D PICTURE IN PICTURE



Why not play games everywhere?

APP SWITCHER



Instagram App Switcher "widget" Prototype

APP SWITCHER WIDGET

- Accomplished with UIApplication...
 - spam app screenshot refreshes with Private API
 - `-[UIApplication _saveSnapshotWithName:]`
 - secret parameter:
`@"UIApplicationAutomaticSnapshotDefault"`

SPRINGBOARD WIDGETS

- can't really draw dynamic icons :(
- can update notifications / application badge
 - let's abuse that!
 - a lot!



INTRODUCING
FANCY LEVEL



FANCY LEVEL

- I've always wanted a leveling app
 - extremely useful when placing paintings
 - but I don't want to open the app (all the time)
- there's totally not a million of them in the App Store
 - let's make one anyways

PROBLEM

- CoreMotion doesn't work in the background :/
- how can we fix this?
 - any takers?

UIKIT + CLASSEDUMP

- UIApplication has lots of fun stuff
 - - [UIApplication **setApplicationBadgeString:**]
 - super secret
 - we can use this to make the icon dynamic

WATCHDOG

- when you close an application on iOS, it goes to the background
 - thanks to watchdogd
 - how do we keep an app open forever?
 - hax.



MUSIC



(THE) SILENCE

- we can play an empty wav file forever
 - iOS "thinks" we're playing music
 - really we're just wasting the battery :P
 - this is actually a really common hack



BACKGROUNDING HAX

- register for audio playback background mode
- play music
- music keeps the app running in the background
- whenever we get device motion data, update the badge
- tada!

:D

DEMO



TOUCH IT

3D TOUCH



IPHONE 6S+ HD WITH 3D TOUCH

- a week ago Apple announced 3D touch
 - we don't have any iPhone 6S's (6Ses?) (success?)
 - it seems pretty cool
 - let's fake it... and make it! :D





(The best Google image result for UITouch... ever)

UITOUCH

- @property (readonly) float **pressure**
- UITapGestureRecognizer has had this for years...
 - it doesn't work anymore :(
- -[UITouch **majorRadius**] is now a thing! (as of iOS 8)
 - -[UITouch **majorRadius**] returns the radius of the touch

UITOUCH (GARAGEBAND)



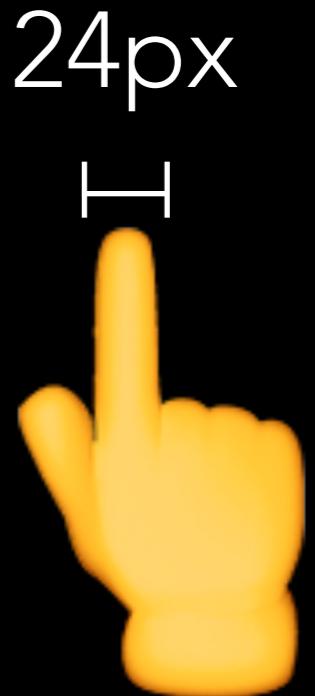
- fun fact:
 - Garageband had pressure sensitivity on its instruments (velocity)
 - was accomplished using the device microphone to listen for louder or softer taps
 - also used the accelerometer (like 3D touch!)

3D TOUCH GESTURE RECOGNIZER

- when a finger is pushed on the screen, it flattens
 - flatter finger —→ larger surface area
 - larger surface area —→ larger touch radius
- 1.0 is a normal press
- >1.0 is a press with more force (scale unbound)

3D TOUCH GESTURE RECOGNIZER

- example (my hand)
 - a normal touch is ~24px in size
 - 1.0 is the current "depth"
 - press harder, touch will grow to ~38px
 - 58% increase, 1.58 would be the new "depth"



HAPTIC, TAPTIC, TOMATO, TOMATO

- Taptic Feedback™ comes with 3D touch
- same as  WATCH
- can't really replicate it
 - but we can fake it using haptics!

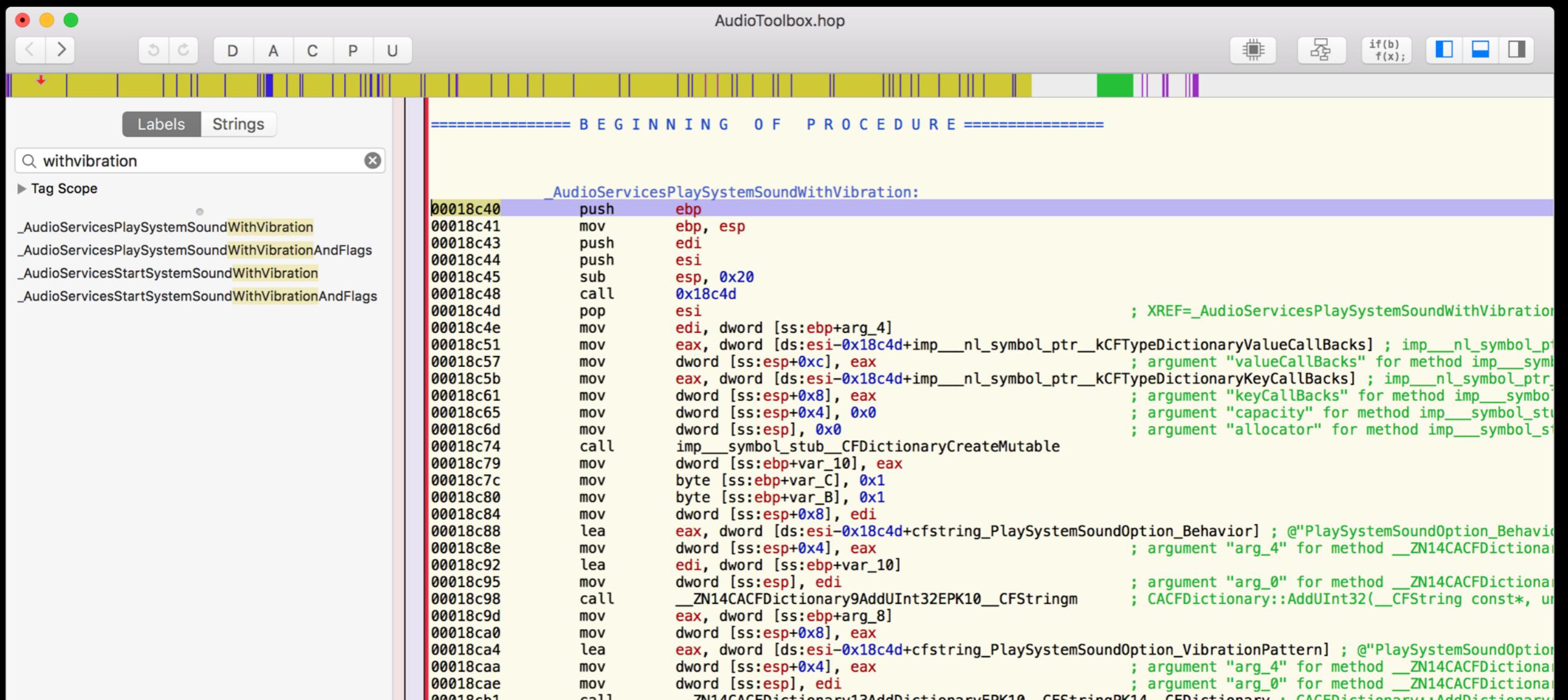


AUDIO SERVICES

- `AudioServicesPlayAlertSound(kSystemSoundID_Vibrate)`
 - too long, 0.2s
- let's find something else...
 - c function, class-dump won't work
 - let's open Hopper!

AUDIO TOOLBOX

- disassembling AudioToolbox gives us something
 - `AudioServicesPlaySystemSoundWithVibration()`



The screenshot shows the Hopper Disassembler interface with the file `AudioToolbox.hop` open. The assembly code for the `AudioServicesPlaySystemSoundWithVibration` procedure is displayed. The code uses standard x86 assembly syntax with registers like `ebp`, `esp`, `edi`, `esi`, and `eax`. It includes memory operations like `push`, `mov`, and `call`. The comments in the assembly code provide context for the arguments being passed to various functions, such as `CFDictionaryCreateMutable` and `CACFDictionary::AddUInt32`. The Hopper interface also shows a sidebar with labels and strings, and a search bar at the top.

```
===== BEGINNING OF PROCEDURE =====

    _AudioServicesPlaySystemSoundWithVibration:
00018c40    push    ebp
00018c41    mov     ebp, esp
00018c43    push    edi
00018c44    push    esi
00018c45    sub     esp, 0x20
00018c48    call    0x18c4d
00018c4d    pop     esi
00018c4e    mov     edi, dword [ss:ebp+arg_4]
00018c51    mov     eax, dword [ds:esi-0x18c4d+imp__nl_symbol_ptr_kCFTypeDictionaryValueCallBacks] ; imp__nl_symbol_p
00018c57    mov     dword [ss:esp+0xc], eax ; argument "valueCallBacks" for method imp__symbol_
00018c5b    mov     eax, dword [ds:esi-0x18c4d+imp__nl_symbol_ptr_kCFTypeDictionaryKeyCallBacks] ; imp__nl_symbol_ptr_
00018c61    mov     dword [ss:esp+0x8], eax ; argument "keyCallBacks" for method imp__symbol_
00018c65    mov     dword [ss:esp+0x4], 0x0 ; argument "capacity" for method imp__symbol_
00018c6d    mov     dword [ss:esp], 0x0 ; argument "allocator" for method imp__symbol_
00018c74    call    imp__symbol_stub_CFDictionaryCreateMutable
00018c79    mov     dword [ss:ebp+var_10], eax
00018c7c    mov     byte [ss:ebp+var_C], 0x1
00018c80    mov     byte [ss:ebp+var_B], 0x1
00018c84    mov     dword [ss:esp+0x8], edi
00018c88    lea     eax, dword [ds:esi-0x18c4d+cfcstring_PlaySystemSoundOption_Behavior] ; @"PlaySystemSoundOption_Behavior"
00018c8e    mov     dword [ss:esp+0x4], eax ; argument "arg_4" for method __ZN14CACFDictiona
00018c92    lea     edi, dword [ss:ebp+var_10]
00018c95    mov     dword [ss:esp], edi
00018c98    call    __ZN14CACFDictiona9AddUInt32EPK10__CFStringm ; argument "arg_0" for method __ZN14CACFDictiona
00018ca0    mov     eax, dword [ss:ebp+arg_8]
00018ca4    mov     dword [ss:esp+0x8], eax
00018caa    lea     eax, dword [ds:esi-0x18c4d+cfcstring_PlaySystemSoundOption_VibrationPattern] ; @"PlaySystemSoundOption_VibrationPattern"
00018cae    mov     dword [ss:esp+0x4], eax ; argument "arg_4" for method __ZN14CACFDictiona
00018cb1    mov     dword [ss:esp], edi ; argument "arg_0" for method __ZN14CACFDictiona
00018cb5    call    __ZN14CACFDictiona13AddDictionaryEPK10__CFStringPK14__CFDictionary ; CACFDictiona::AddDictionary
```

AUDIO SERVICES

let's implement that...

tldr:

```
24 void PDPpseudo3DTouchPlayTap() {
25     NSArray *vibrationPattern = @[
26         @YES,    // YES to vibrate
27         @100,   // 100ms
28     ];
29
30     NSDictionary *dictionary = @{
31         @"Intensity" : @1.0,
32         @"VibePattern" : vibrationPattern,
33     };
34
35     AudioServicesPlaySystemSoundWithVibration(0xFFFF, nil, dictionary);
36 }
```

:D

DEMO



this is what a hacker looks like... apparently...

SUMMARY

- do use/explore Private API to make cool demos
 - abuse it when you can!
- don't ship Private API code publicly
- do make really awesome prototypes
- don't say no because something is difficult
- do act ahead of the curve
- do make cool stuff

“A smile is a curve that sets everything straight.”

-PHYLLIS DILLER

:)

QUESTIONS?