INSPECTING 3RD PARTY APPS

I'M STAN!

A.K.A @LXCID

DISCLAIMER

FOR EDUCATION PURPOSE ONLY

ATTACK SURFACE

APP CONTENT

EXTRACTION

APP CONTENT EXTRACTION

- DOWNLOAD APP USING ITUNES.
- RIGHT CLICK ON THE APP AND SELECT SHOW IN FINDER.
- RENAME THE `.ipa` FILE TO `.zip` FILE.
- EXTRACTS THE ZIP FILE.
- FIND THE APP PACKAGE IN `Payload` DIRECTORY.
- RIGHT CLICK ON THE APP AND SELECT SHOW PACKAGE CONTENTS.

APP CONTENT

EXTRACTION

GRAB

APP DOCUMENTS

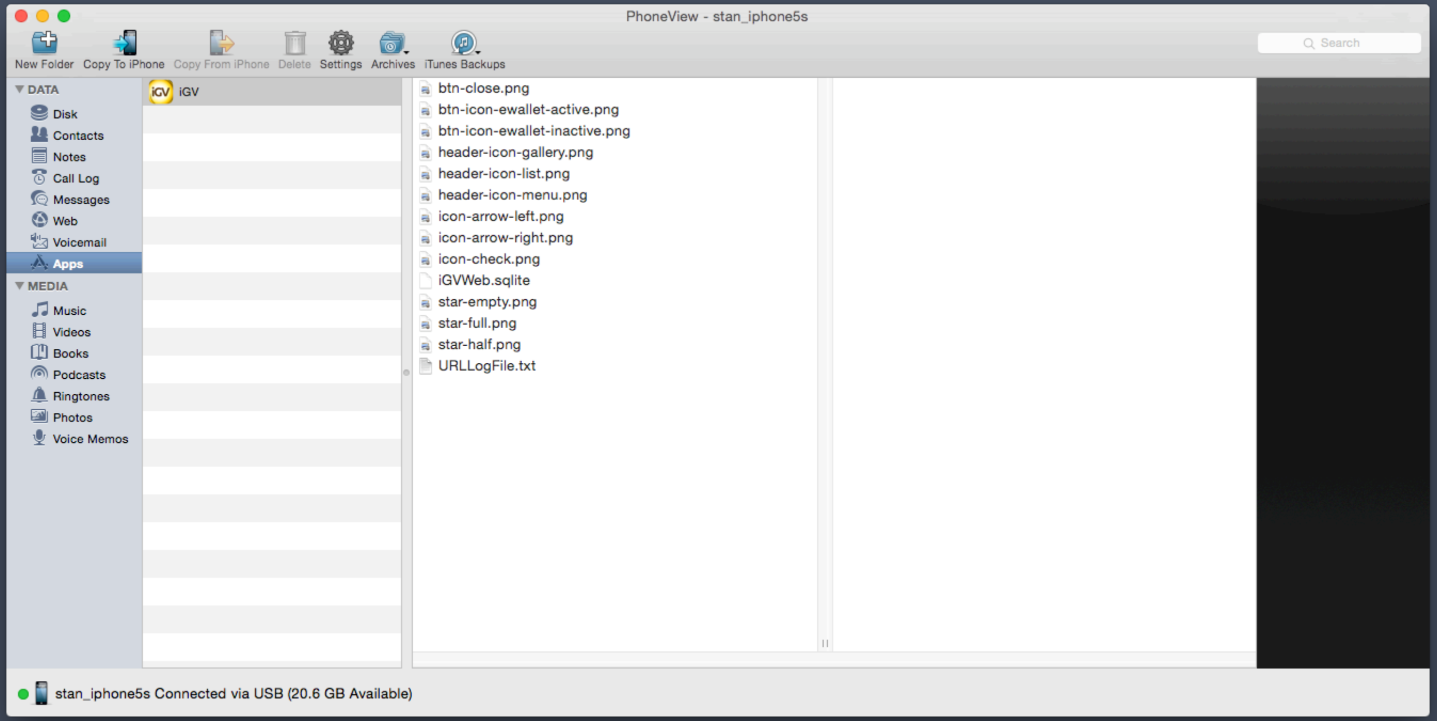
EXTRACTION

APP DOCUMENTS

EXTRACTION

ONLY WORKS BEFORE IOS 8.3

APP DOCUMENTS EXTRACTION



```
btn-close.png
btn-icon-ewallet-active.png
btn-icon-ewallet-inactive.png
header-icon-gallery.png
header-icon-list.png
header-icon-menu.png
icon-arrow-left.png
icon-arrow-right.png
icon-check.png
iGVWeb.sqlite
star-empty.png
star-full.png
star-half.png
URLLogFile.txt
```

stan_iphone5s Connected via USB (20.6 GB Available)

PHONEVIEW, IEXPLORER, ETC…

DANGER: TRUST NO COMPUTER!!!!

NETWORK/API

ANALYSIS

NETWORK/API ANALYSIS

MOTM WITH CHARLES PROXY: CHARLESPROXY.COM

- ENSURE YOUR COMPUTER AND PHONE ARE CONNECTED TO THE SAME WI-FI NETWORK.
- ACCESS THE CONNECTED WI-FI SETTINGS UNDER

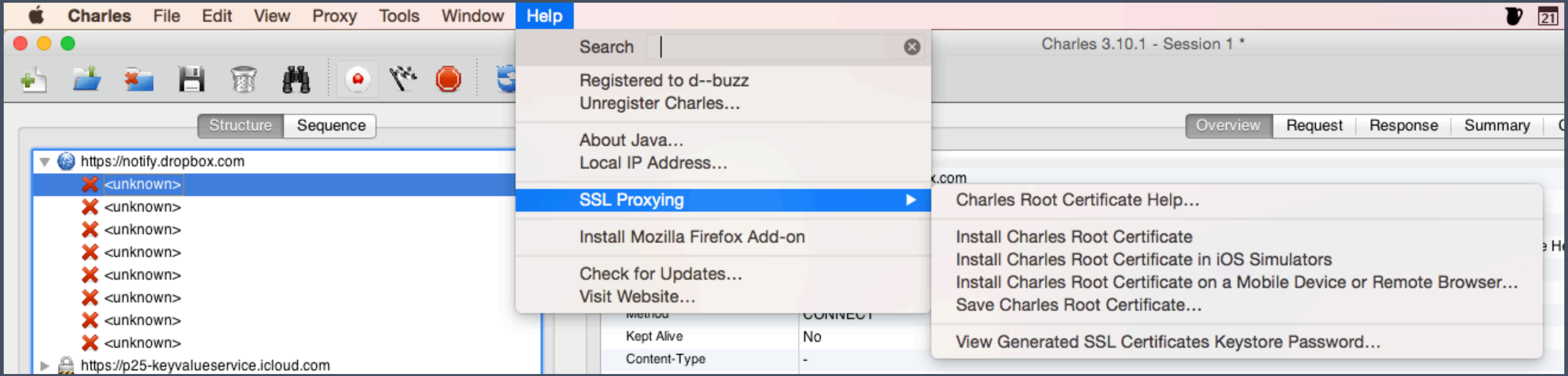
SETTINGS > WI-FI > CONNECTED WI-FI NETWORK NAME

- SET HTTP PROXY TO MANUAL, SERVER AND PORT POINT TO CHARLES PROXY.

SSL

INSTALL ROOT CERTIFICATE.

DANGER: YOU MUST KNOW WHAT YOU DOING



Charles 3.10.1 - Session 1 *

https://notify.dropbox.com

<unknown>
<unknown>
<unknown>
<unknown>
<unknown>
<unknown>
<unknown>
<unknown>

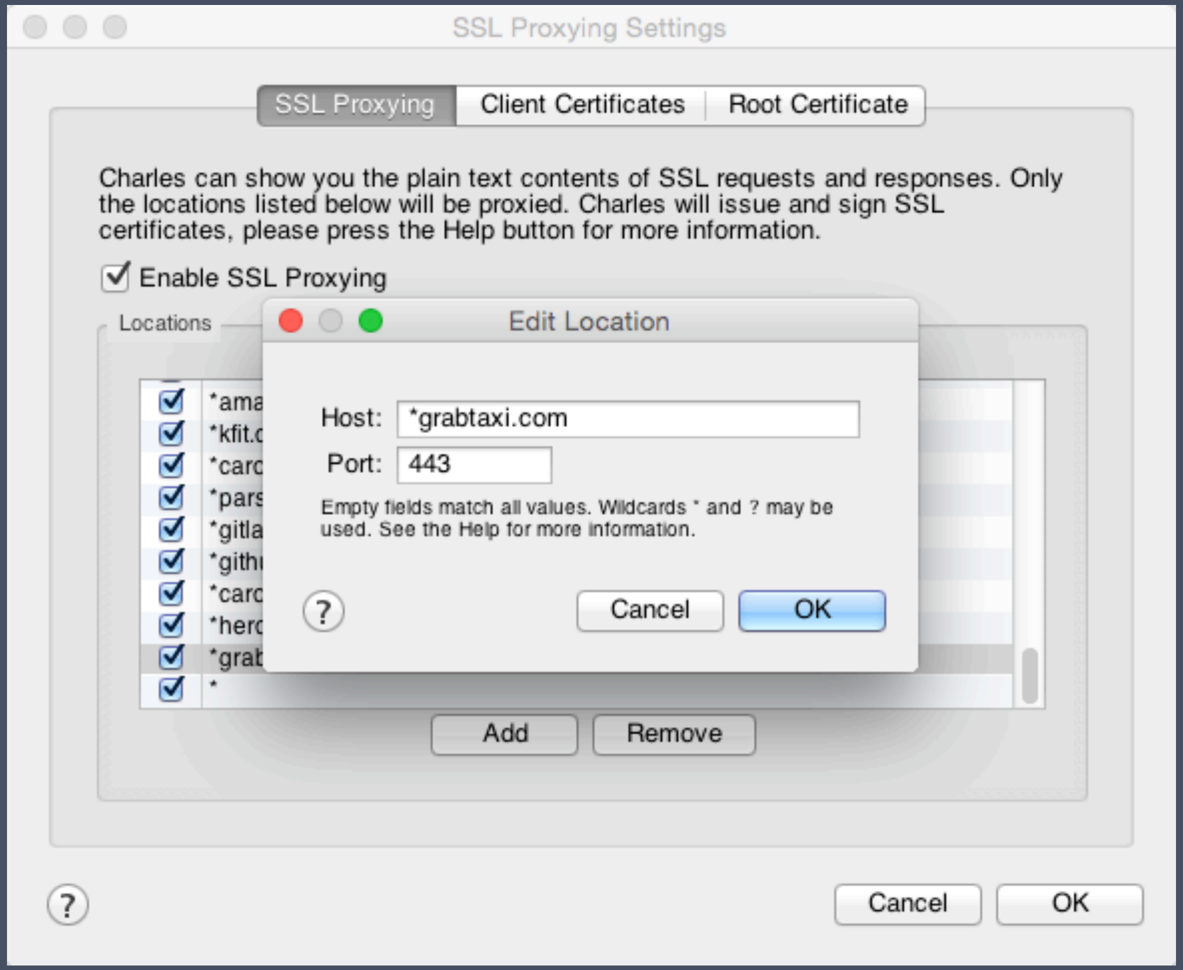
https://p25-keyvalueservice.icloud.com

Method	CONNECT
Kept Alive	No
Content-Type	-

Charles
File
Edit
View
Proxy
Tools
Window
Help
Search
Registered to d--buzz
Unregister Charles…
About Java…
Local IP Address…
SSL Proxying
Install Mozilla Firefox Add-on
Check for Updates…
Visit Website…
Charles Root Certificate Help…
Install Charles Root Certificate
Install Charles Root Certificate in iOS Simulators
Install Charles Root Certificate on a Mobile Device or Remote Browser…
Save Charles Root Certificate…
View Generated SSL Certificates Keystore Password…
Structure
Sequence
Overview
Request
Response
Summary

SSL

GO TO MENU > PROXY > SSL PROXY SETTINGS...



SSL Proxying Settings

Charles can show you the plain text contents of SSL requests and responses. Only the locations listed below will be proxied. Charles will issue and sign SSL certificates, please press the Help button for more information.

☑ Enable SSL Proxying

Locations

☑ *ama
☑ *kfit.c
☑ *carc
☑ *pars
☑ *gitla
☑ *githu
☑ *carc
☑ *herc
☑ *grab
☑ *

Edit Location

Host: *grabtaxi.com

Port: 443

Empty fields match all values. Wildcards * and ? may be used. See the Help for more information.

SSL PINNING

UH-OH

JAILBREAK

REDDIT.COM/R/JAILBREAK

9.0, 9.1, ~~9.2~~

LOTS OF GREAT CONTENT OUT THE NET

- REALM.IO: REVERSE-ENGINEERING IOS APPS: HACKING ON LYFT
- JAILBREAKCON 2013 - ADAM BELL
- PETER STEINBERGER: HOW TO INSPECT THE VIEW HIERARCHY OF THIRD-PARTY APPS
- IPHONEDEVWIKI: REVERSE ENGINEERING TOOLS

DETOUR

APP DOCUMENTS EXTRACTION

/W SSH

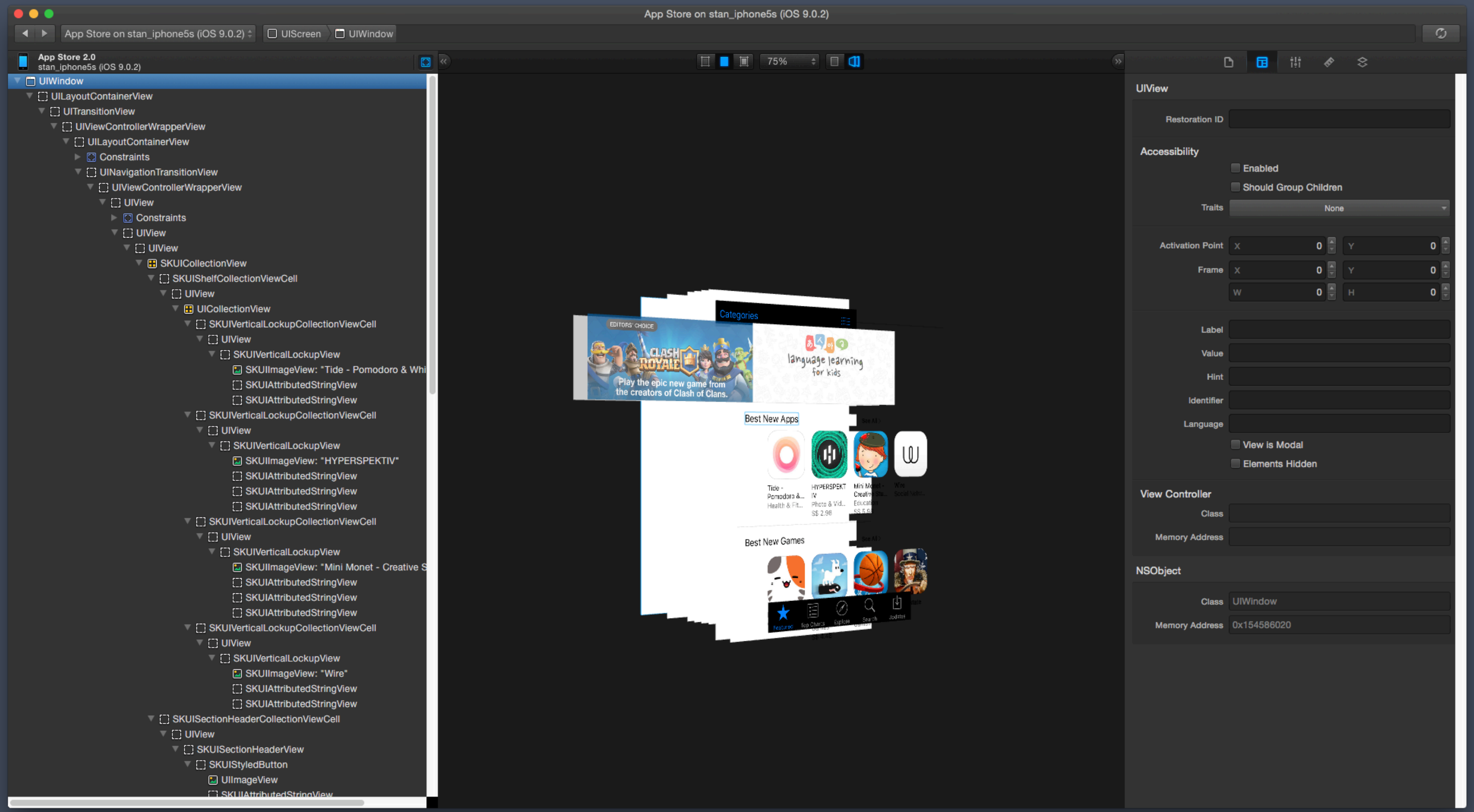
DATA: /PRIVATE/VAR/MOBILE/CONTAINERS/DATA/{UUID}

APP GROUP: /PRIVATE/VAR/MOBILE/CONTAINERS/SHARED/APPGROUP/{UUID}

VIEW HIERARCHY

INSPECTION

VIEW HIERARCHY INSPECTION /W REVEAL



App Store on stan_iphone5s (iOS 9.0.2)

App Store on stan_iphone5s (iOS 9.0.2) | UIScreen | UIWindow

App Store 2.0
stan_iphone5s (iOS 9.0.2)

```
UIWindow
  UILayoutContainerView
    UITransitionView
      UIViewControllerWrapperView
        UILayoutContainerView
          Constraints
          UINavigationTransitionView
            UIViewControllerWrapperView
              UIView
                Constraints
                UIView
                  UIView
                    SKUICollectionView
                      SKUIShelfCollectionViewCell
                        UIView
                          UICollectionView
                            SKUIVerticalLockupCollectionViewCell
                              UIView
                                SKUIVerticalLockupView
                                  SKUIImageView: "Tide - Pomodoro & Whi
                                  SKUIAttributedStringView
                                  SKUIAttributedStringView
                            SKUIVerticalLockupCollectionViewCell
                              UIView
                                SKUIVerticalLockupView
                                  SKUIImageView: "HYPERSPEKTIV"
                                  SKUIAttributedStringView
                                  SKUIAttributedStringView
                                  SKUIAttributedStringView
                            SKUIVerticalLockupCollectionViewCell
                              UIView
                                SKUIVerticalLockupView
                                  SKUIImageView: "Mini Monet - Creative S
                                  SKUIAttributedStringView
                                  SKUIAttributedStringView
                                  SKUIAttributedStringView
                            SKUIVerticalLockupCollectionViewCell
                              UIView
                                SKUIVerticalLockupView
                                  SKUIImageView: "Wire"
                                  SKUIAttributedStringView
                                  SKUIAttributedStringView
                      SKUISectionHeaderCollectionViewCell
                        UIView
                          SKUISectionHeaderView
                            SKUIStyledButton
                              UIImageView
                              SKUIAttributedStringView
```

UIView

Restoration ID

Accessibility

□ Enabled

□ Should Group Children

Traits: None

Activation Point: X 0, Y 0

Frame: X 0, Y 0, W 0, H 0

Label

Value

Hint

Identifier

Language

□ View is Modal

□ Elements Hidden

View Controller

Class

Memory Address

NSObject

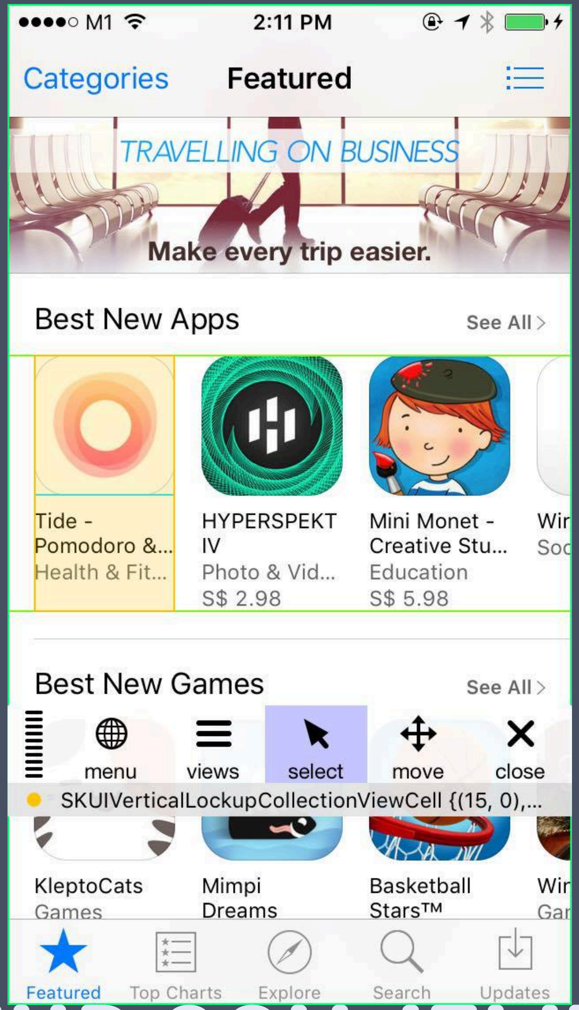
Class: UIWindow

Memory Address: 0x154586020

HTTP://REVEALAPP.COM

HTTPS://GITHUB.COM/HEARDRWT/REVEALLOADER

VIEW HIERARCHY INSPECTION /W FLEX



SKUIVerticalLockupCollectionViewCell {(15, 0),...

HTTPS://GITHUB.COM/FLIPBOARD/FLEX

HTTPS://GITHUB.COM/QIAOXUESHI/FLEXLOADER

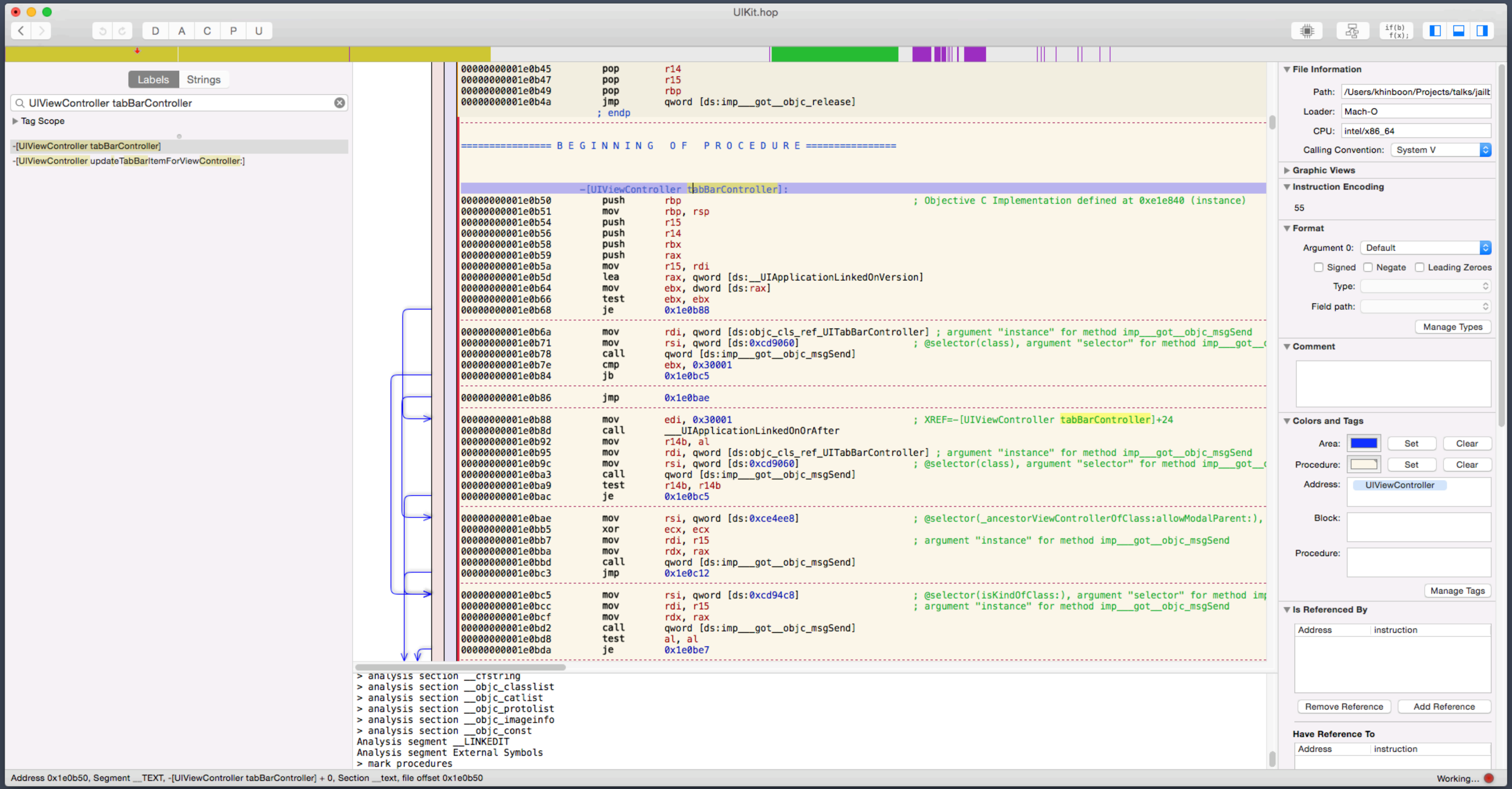
DETOUR

BREAKING SSL PINNING

CODE INSPECTION

HOPPER OR IDA PRO

CODE INSPECTION /W HOPPER


UIKit.hop
D
A
C
P
U
Labels
Strings
UIViewController tabBarController
Tag Scope
-[UIViewController tabBarController]
-[UIViewController updateTabBarItemForViewController:]

```
00000000001e0b45        pop        r14
00000000001e0b47        pop        r15
00000000001e0b49        pop        rbp
00000000001e0b4a        jmp        qword [ds:imp___got__objc_release]
                      ; endp

================ B E G I N N I N G   O F   P R O C E D U R E ================


                -[UIViewController tabBarController]:
00000000001e0b50        push       rbp                                     ; Objective C Implementation defined at 0xe1e840 (instance)
00000000001e0b51        mov        rbp, rsp
00000000001e0b54        push       r15
00000000001e0b56        push       r14
00000000001e0b58        push       rbx
00000000001e0b59        push       rax
00000000001e0b5a        mov        r15, rdi
00000000001e0b5d        lea        rax, qword [ds:__UIApplicationLinkedOnVersion]
00000000001e0b64        mov        ebx, dword [ds:rax]
00000000001e0b66        test       ebx, ebx
00000000001e0b68        je         0x1e0b88

00000000001e0b6a        mov        rdi, qword [ds:objc_cls_ref_UITabBarController] ; argument "instance" for method imp___got__objc_msgSend
00000000001e0b71        mov        rsi, qword [ds:0xcd9060]                ; @selector(class), argument "selector" for method imp___got__
00000000001e0b78        call       qword [ds:imp___got__objc_msgSend]
00000000001e0b7e        cmp        ebx, 0x30001
00000000001e0b84        jb         0x1e0bc5

00000000001e0b86        jmp        0x1e0bae

00000000001e0b88        mov        edi, 0x30001                            ; XREF=-[UIViewController tabBarController]+24
00000000001e0b8d        call       ___UIApplicationLinkedOnOrAfter
00000000001e0b92        mov        r14b, al
00000000001e0b95        mov        rdi, qword [ds:objc_cls_ref_UITabBarController] ; argument "instance" for method imp___got__objc_msgSend
00000000001e0b9c        mov        rsi, qword [ds:0xcd9060]                ; @selector(class), argument "selector" for method imp___got__
00000000001e0ba3        call       qword [ds:imp___got__objc_msgSend]
00000000001e0ba9        test       r14b, r14b
00000000001e0bac        je         0x1e0bc5

00000000001e0bae        mov        rsi, qword [ds:0xce4ee8]                ; @selector(_ancestorViewControllerOfClass:allowModalParent:),
00000000001e0bb5        xor        ecx, ecx
00000000001e0bb7        mov        rdi, r15                                ; argument "instance" for method imp___got__objc_msgSend
00000000001e0bba        mov        rdx, rax
00000000001e0bbd        call       qword [ds:imp___got__objc_msgSend]
00000000001e0bc3        jmp        0x1e0c12

00000000001e0bc5        mov        rsi, qword [ds:0xcd94c8]                ; @selector(isKindOfClass:), argument "selector" for method imp
00000000001e0bcc        mov        rdi, r15                                ; argument "instance" for method imp___got__objc_msgSend
00000000001e0bcf        mov        rdx, rax
00000000001e0bd2        call       qword [ds:imp___got__objc_msgSend]
00000000001e0bd8        test       al, al
00000000001e0bda        je         0x1e0be7
```

```
> analysis section __cfstring
> analysis section __objc_classlist
> analysis section __objc_catlist
> analysis section __objc_protolist
> analysis section __objc_imageinfo
> analysis section __objc_const
Analysis segment __LINKEDIT
Analysis segment External Symbols
> mark procedures
```

Address 0x1e0b50, Segment __TEXT, -[UIViewController tabBarController] + 0, Section __text, file offset 0x1e0b50

▼ File Information

Path: /Users/khinboon/Projects/talks/jailt

Loader: Mach-O

CPU: intel/x86_64

Calling Convention: System V

▶ Graphic Views

▼ Instruction Encoding

55

▼ Format

Argument 0: Default

□ Signed □ Negate □ Leading Zeroes

Type:

Field path:

Manage Types

▼ Comment

▼ Colors and Tags

Area: 🟦 Set Clear

Procedure: Set Clear

Address: UIViewController

Block:

Procedure:

Manage Tags

▼ Is Referenced By

Address	instruction

Remove Reference Add Reference

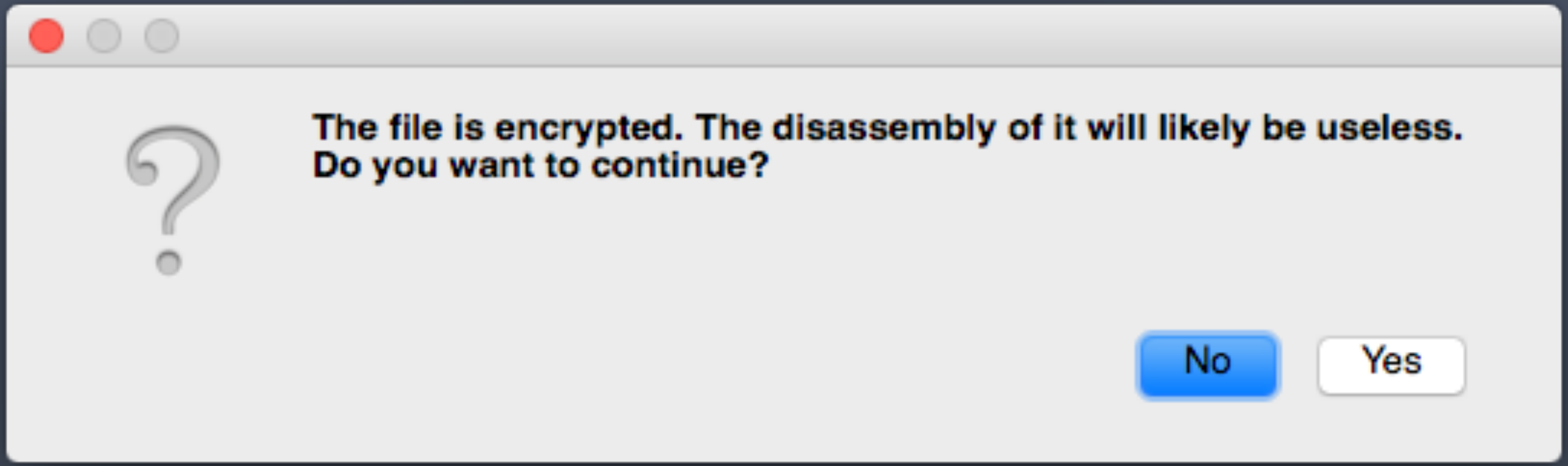
Have Reference To

Address	instruction

Working...

APPS FROM ITUNES

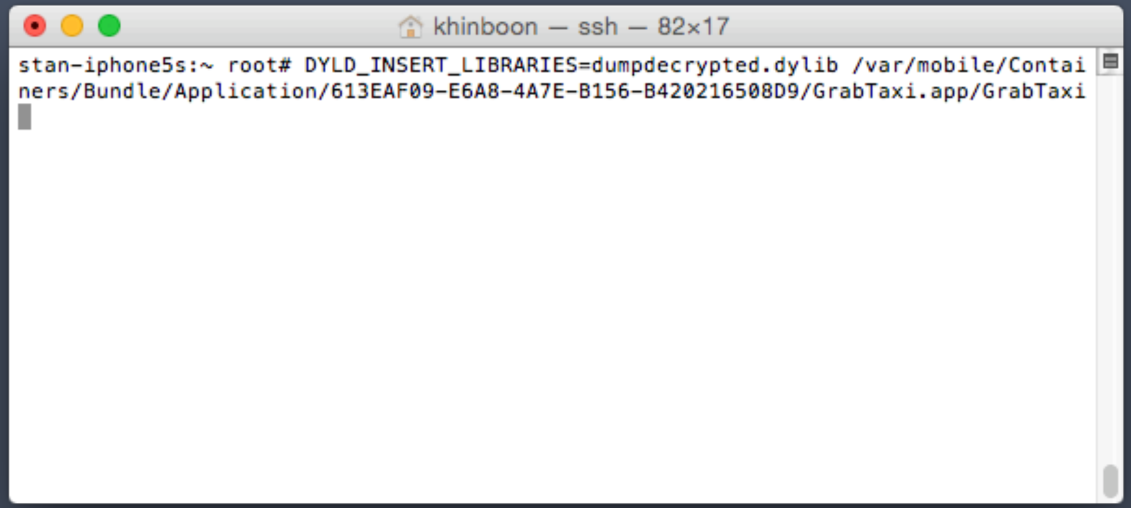
ARE ENCRYPTED



The file is encrypted. The disassembly of it will likely be useless.
Do you want to continue?

DUMPDECRYPT

```
DYLD_INSERT_LIBRARIES=dumpdecrypted.dylib /var/mobile/
Containers/Bundle/Application/*/GrabTaxi.app/GrabTaxi
```



```
stan-iphone5s:~ root# DYLD_INSERT_LIBRARIES=dumpdecrypted.dylib /var/mobile/Contai
ners/Bundle/Application/613EAF09-E6A8-4A7E-B156-B420216508D9/GrabTaxi.app/GrabTaxi
```

HTTPS://GITHUB.COM/STEFANESSER/DUMPDECRYPTED

CODE

INJECTION

CYCRIPT

INSPIRED BY...

- SINGAPORE TAXIS
- FOSS ASIA 2016: UNCOVERING OF AN OBFUSCATED PUBLIC GOVERNMENTAL API

CASE STUDY

CRACKING TAXI-TAXI@SG'S PASSWORD

MORE WE HAVE NOT TALKED ABOUT...

- LLDB
- CLASS DUMP
- TWEAKS

THANK YOU!