TrustKit

Code Injection on iOS 8 for the Greater Good

Alban Diquet - @nabla_c0d3
Angela Chow - @paranoid_angela
Eric Castro - @_eric_castro

black hat
USA 2015

About Us

- Alban: Engineering/security lead at Data Theorem
- Eric: iOS R&D at Data Theorem
- Angela: Paranoids (security) at Yahoo

How It All Started

- iOS 8 released: dynamic libraries now allowed in App Store Apps!

How It All Started

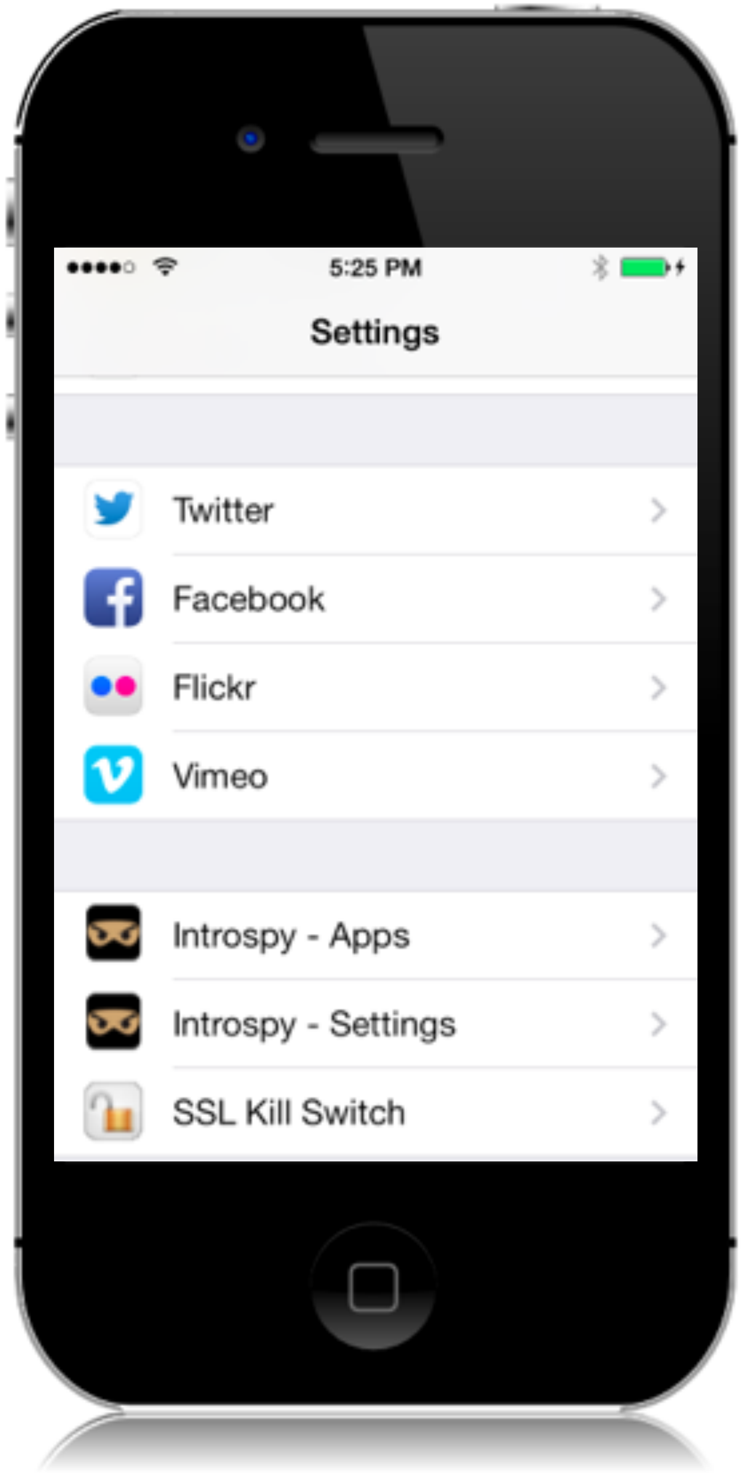
- iOS 8 released: dynamic libraries now allowed in App Store Apps!
- Lot of experience building Cydia “tweaks”, which are dylibs

How It All Started

- iO mic libraries now allowed in
  Ap
- Lo lding Cydia “tweaks”, which
  are

How It All Started

- iO mic libr in
  Ap
- Lo lding C ch
  are


5:25 PM

Settings

Twitter

Facebook

Flickr

Vimeo

Introspy - Apps

Introspy - Settings

SSL Kill Switch

How It All Started

- iOS 8 released: dynamic libraries now allowed in App Store Apps!

- Lot of experience building Cydia “tweaks”, which are dylibs

How It All Started

- iOS 8 released: dynamic libraries now allowed in App Store Apps!
- Lot of experience building Cydia "tweaks", which are dylibs
- At the time, we were thinking about building an open-source SSL pinning library

How It All Started

- iOS 8 released: dynamic libraries now allowed in App Store Apps!
- Lot of experience building Cydia “tweaks”, which are dylibs
- At the time, we were thinking about building an open-source SSL pinning library
- Can we create an SSL pinning tweak and package it in an App Store App on a non-jailbroken device?

How It All Started

- iOS 8 released: dynamic libraries now allowed in App Store Apps!
- Lot of experience building Cydia “tweaks”, which are dylibs
- At the time, we were thinking about building an open-source SSL pinning library
- Can we create an SSL pinning tweak and package it in an App Store App on a non-jailbroken device?

Agenda

- Dynamic Libraries and iOS 8
- Cydia Substrate on a Non-Jailbroken Device
- Putting It All Together: TrustKit

Agenda

- Dynamic Libraries and iOS 8
- Cydia Substrate on a Non-Jailbroken Device
- Putting It All Together: TrustKit

Dylibs Before iOS 8

- Historically: no third-party dynamic libraries in Apps
    - System dylibs packaged with the OS

Dylibs Before iOS 8

- Historically: no third-party dynamic libraries in Apps
  - System dylibs packaged with the OS
- Developer libraries: static linking only
  - Enforced via the App Store review process
  - Made library distribution complex (see: CocoaPods)
  - Security decision ?

Dylibs on iOS 8

- iOS 8: dynamic libraries now accepted
    - Apple calls them “Embedded Frameworks”
- Introduced to facilitate sharing code between Apps and their App Extensions
    - But… can be used regardless of whether the App actually has an Extension

Dylibs on iOS 8

- Mach-O is the file format for OS X and iOS programs and libraries.
- Executables interact with “dyld”, the OS X and iOS dynamic linker to load libraries at runtime.
- A dynamic library is described in Mach-O binary in a “load command” structure

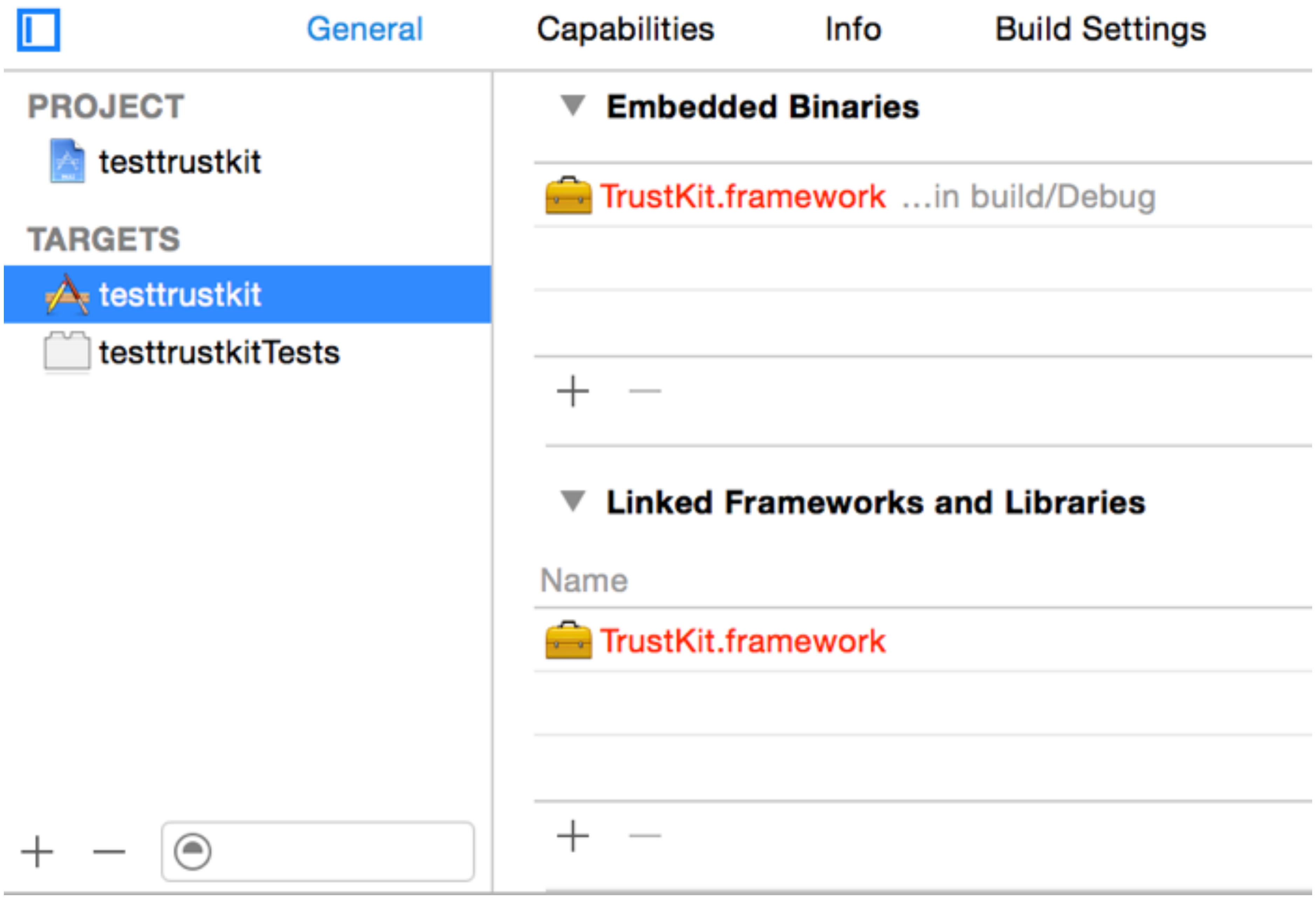
Dylibs on iOS 8

- Sandboxing requires that libraries are packaged within the app’s bundle
  - Unlike Substrate tweaks which are stored in */Library/*

Dylibs on iOS 8

- Sandboxing requires that libraries are packaged within the app's bundle
  - Unlike Substrate tweaks which are stored in */Library/*
- **dyld** locates them through relative paths
  - **@executable_path** prefix allows to locate libraries in paths relative to the main executable.
  - **@rpath** prefix allows for multiple library search locations.
    - In iOS, @rpath seems limited to one single location ("Frameworks" directory inside app's bundle)

Dylibs on iOS 8

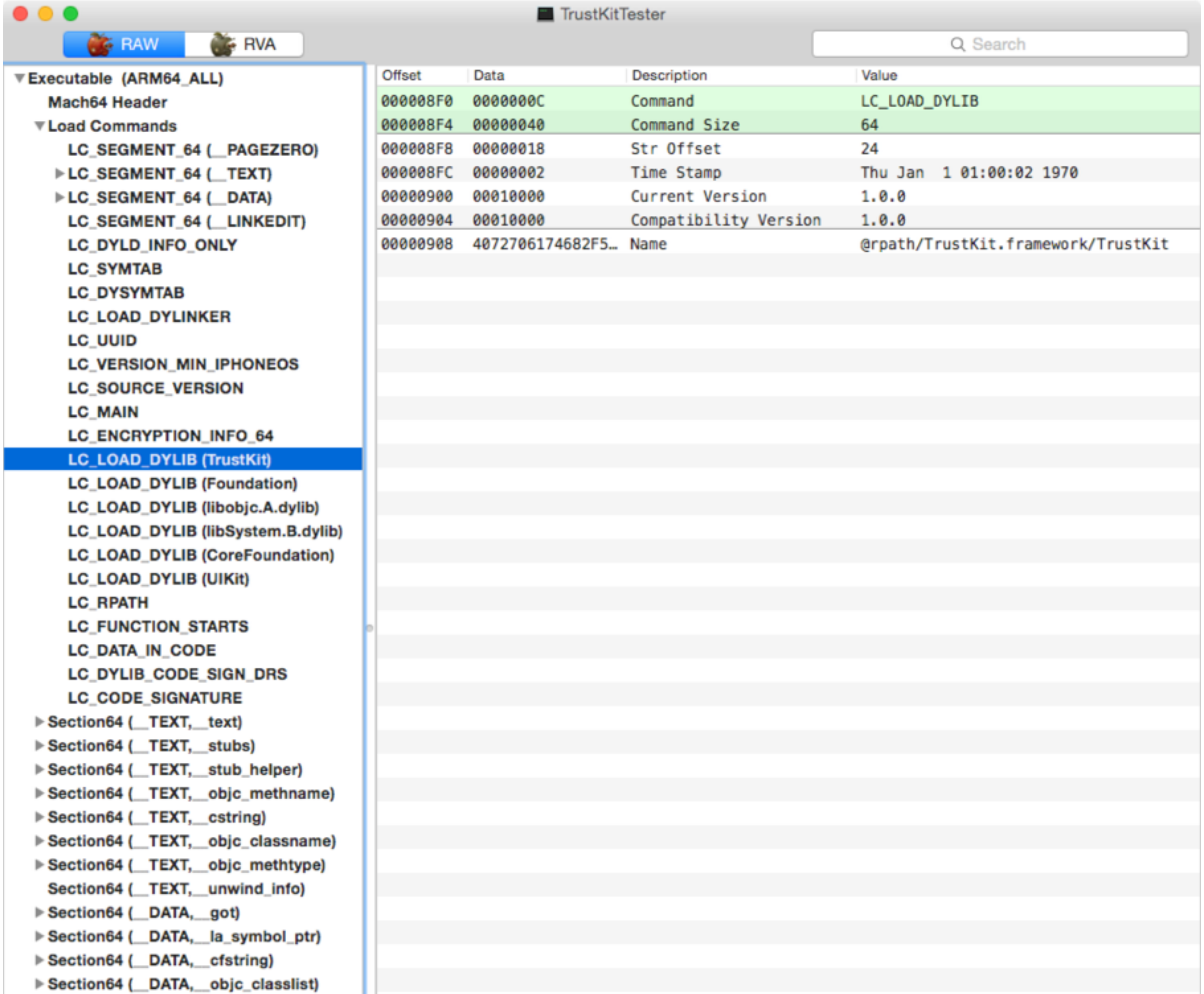


Embedded Binaries

TrustKit.framework ...in build/Debug

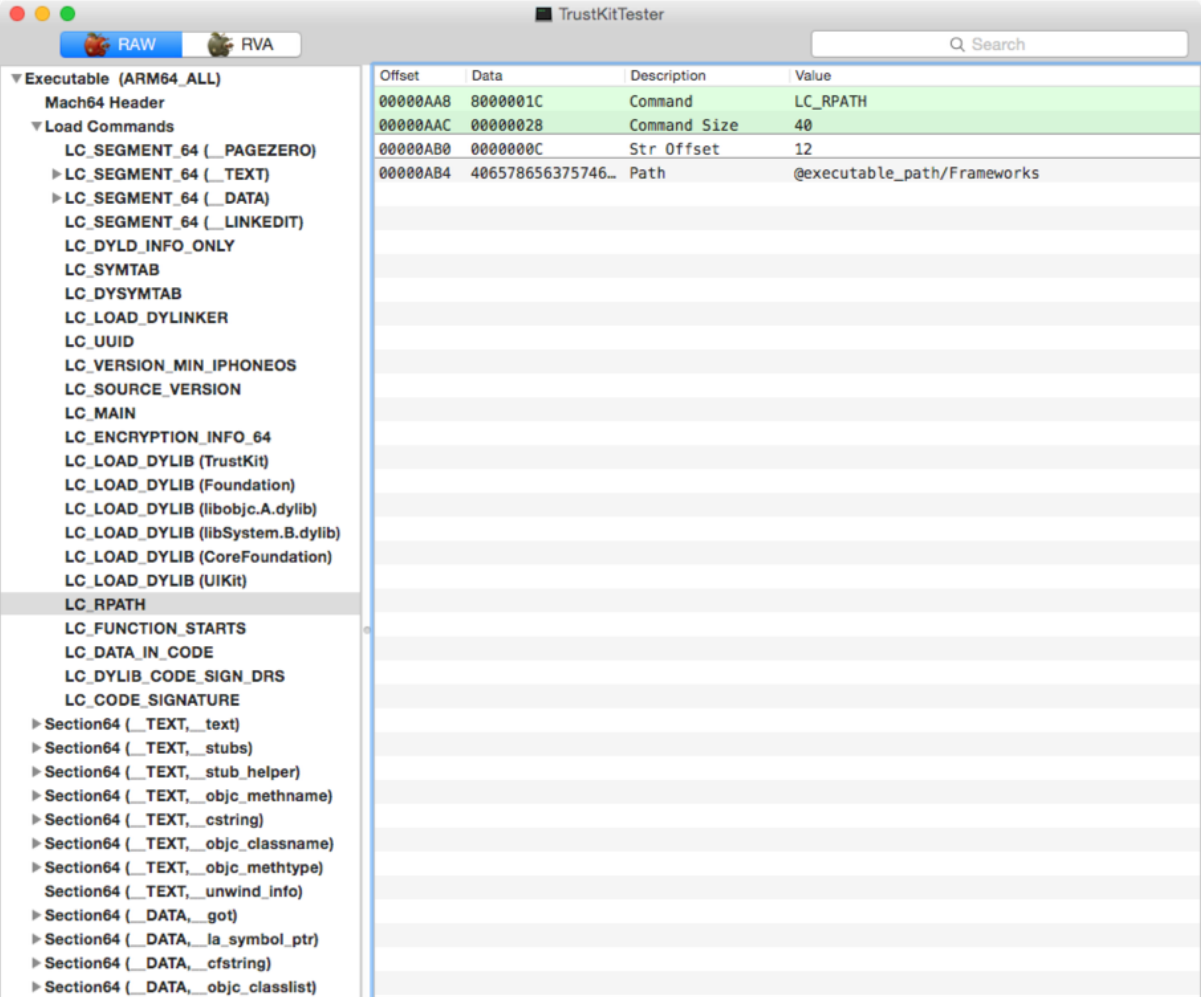
Linked Frameworks and Libraries

Name
TrustKit.framework



```
▼ Executable (ARM64_ALL)
    Mach64 Header
  ▼ Load Commands
      LC_SEGMENT_64 (__PAGEZERO)
    ▶ LC_SEGMENT_64 (__TEXT)
    ▶ LC_SEGMENT_64 (__DATA)
      LC_SEGMENT_64 (__LINKEDIT)
      LC_DYLD_INFO_ONLY
      LC_SYMTAB
      LC_DYSYMTAB
      LC_LOAD_DYLINKER
      LC_UUID
      LC_VERSION_MIN_IPHONEOS
      LC_SOURCE_VERSION
      LC_MAIN
      LC_ENCRYPTION_INFO_64
      LC_LOAD_DYLIB (TrustKit)
      LC_LOAD_DYLIB (Foundation)
      LC_LOAD_DYLIB (libobjc.A.dylib)
      LC_LOAD_DYLIB (libSystem.B.dylib)
      LC_LOAD_DYLIB (CoreFoundation)
      LC_LOAD_DYLIB (UIKit)
      LC_RPATH
      LC_FUNCTION_STARTS
      LC_DATA_IN_CODE
      LC_DYLIB_CODE_SIGN_DRS
      LC_CODE_SIGNATURE
  ▶ Section64 (__TEXT,__text)
  ▶ Section64 (__TEXT,__stubs)
  ▶ Section64 (__TEXT,__stub_helper)
  ▶ Section64 (__TEXT,__objc_methname)
  ▶ Section64 (__TEXT,__cstring)
  ▶ Section64 (__TEXT,__objc_classname)
  ▶ Section64 (__TEXT,__objc_methtype)
    Section64 (__TEXT,__unwind_info)
  ▶ Section64 (__DATA,__got)
  ▶ Section64 (__DATA,__la_symbol_ptr)
  ▶ Section64 (__DATA,__cfstring)
  ▶ Section64 (__DATA,__objc_classlist)
```

Offset	Data	Description	Value
000008F0	0000000C	Command	LC_LOAD_DYLIB
000008F4	00000040	Command Size	64
000008F8	00000018	Str Offset	24
000008FC	00000002	Time Stamp	Thu Jan 1 01:00:02 1970
00000900	00010000	Current Version	1.0.0
00000904	00010000	Compatibility Version	1.0.0
00000908	4072706174682F5…	Name	@rpath/TrustKit.framework/TrustKit



- Executable (ARM64_ALL)
  - Mach64 Header
  - Load Commands
    - LC_SEGMENT_64 (__PAGEZERO)
    - LC_SEGMENT_64 (__TEXT)
    - LC_SEGMENT_64 (__DATA)
    - LC_SEGMENT_64 (__LINKEDIT)
    - LC_DYLD_INFO_ONLY
    - LC_SYMTAB
    - LC_DYSYMTAB
    - LC_LOAD_DYLINKER
    - LC_UUID
    - LC_VERSION_MIN_IPHONEOS
    - LC_SOURCE_VERSION
    - LC_MAIN
    - LC_ENCRYPTION_INFO_64
    - LC_LOAD_DYLIB (TrustKit)
    - LC_LOAD_DYLIB (Foundation)
    - LC_LOAD_DYLIB (libobjc.A.dylib)
    - LC_LOAD_DYLIB (libSystem.B.dylib)
    - LC_LOAD_DYLIB (CoreFoundation)
    - LC_LOAD_DYLIB (UIKit)
    - LC_RPATH
    - LC_FUNCTION_STARTS
    - LC_DATA_IN_CODE
    - LC_DYLIB_CODE_SIGN_DRS
    - LC_CODE_SIGNATURE
  - Section64 (__TEXT,__text)
  - Section64 (__TEXT,__stubs)
  - Section64 (__TEXT,__stub_helper)
  - Section64 (__TEXT,__objc_methname)
  - Section64 (__TEXT,__cstring)
  - Section64 (__TEXT,__objc_classname)
  - Section64 (__TEXT,__objc_methtype)
  - Section64 (__TEXT,__unwind_info)
  - Section64 (__DATA,__got)
  - Section64 (__DATA,__la_symbol_ptr)
  - Section64 (__DATA,__cfstring)
  - Section64 (__DATA,__objc_classlist)

Offset	Data	Description	Value
00000AA8	8000001C	Command	LC_RPATH
00000AAC	00000028	Command Size	40
00000AB0	0000000C	Str Offset	12
00000AB4	406578656375746...	Path	@executable_path/Frameworks

Agenda

- Dynamic Libraries and iOS 8
- Cydia Substrate on a Non-Jailbroken Device
- Putting It All Together: TrustKit

Agenda

- Dynamic Libraries and iOS 8
- Cydia Substrate on a Non-Jailbroken Device
- Putting It All Together: TrustKit

Substrate Tweaks

- So can we package a Substrate tweak in an App?

Substrate Tweaks

- So can we package a Substrate tweak in an App?
  - For testing, tried packaging an existing tweak
    - *ios-ssl-kill-switch*
      - (In)security tool for disabling SSL validation and pinning

Substrate Tweaks

- So can we package a Substrate tweak in an App?
  - For testing, tried packaging an existing tweak
    - *ios-ssl-kill-switch*
      - (In)security tool for disabling SSL validation and pinning
  - If it works, we can build our SSL pinning tweak!

Substrate Tweaks

- What is a Substrate tweak again?

Substrate Tweaks

- What is a Substrate tweak again?
  - Dylib with a constructor to initialize hooks

Substrate Tweaks

- What is a Substrate tweak again?

```
__attribute__((constructor)) static void initialize()
{
    // Our library just got injected in the App - initialize things
    initTweak();
    // ...

    // Enable hooks
    NSLog(@"SSL Kill Switch - Hook Enabled.");
    MSHookFunction((void *) SSLHandshake,
                   (void *) replaced_SSLHandshake,
                   (void **) &original_SSLHandshake);

    MSHookFunction((void *) SSLSetSessionOption,
                   (void *) replaced_SSLSetSessionOption,
                   (void **) &original_SSLSetSessionOption);

    MSHookFunction((void *) SSLCreateContext,
                   (void *) replaced_SSLCreateContext,
                   (void **) &original_SSLCreateContext);
    // ...
    // End of the constructor
}
```

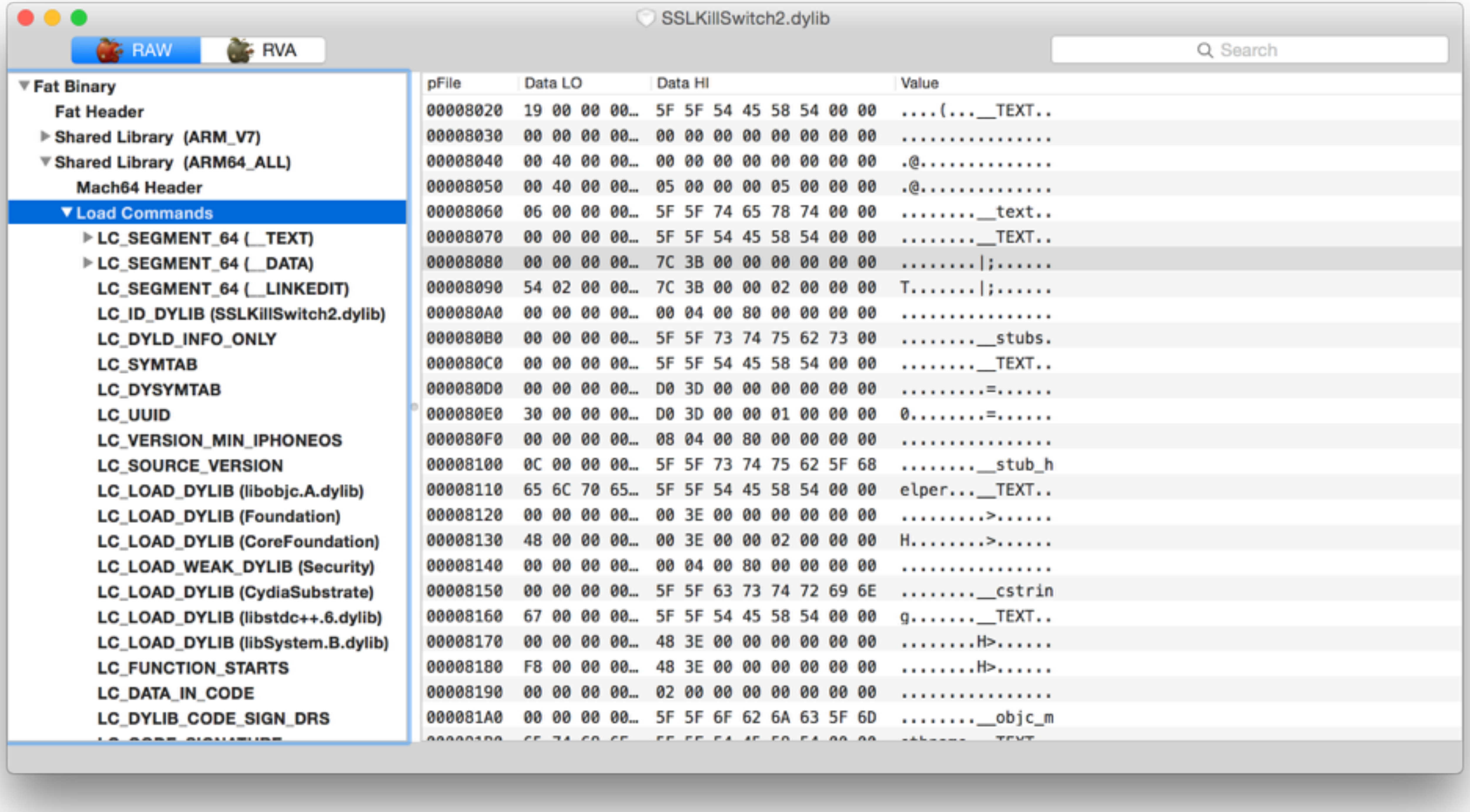
Substrate Tweaks

- What is a Substrate tweak again?
    - Dylib with a constructor to initialize hooks

Substrate Tweaks

- What is a Substrate tweak again?
    - Dylib with a constructor to initialize hooks
    - CydiaSubstrate dylib as a dependency, for calling the hooking functions *MSHookFunction(), MSHookMessageEx()*

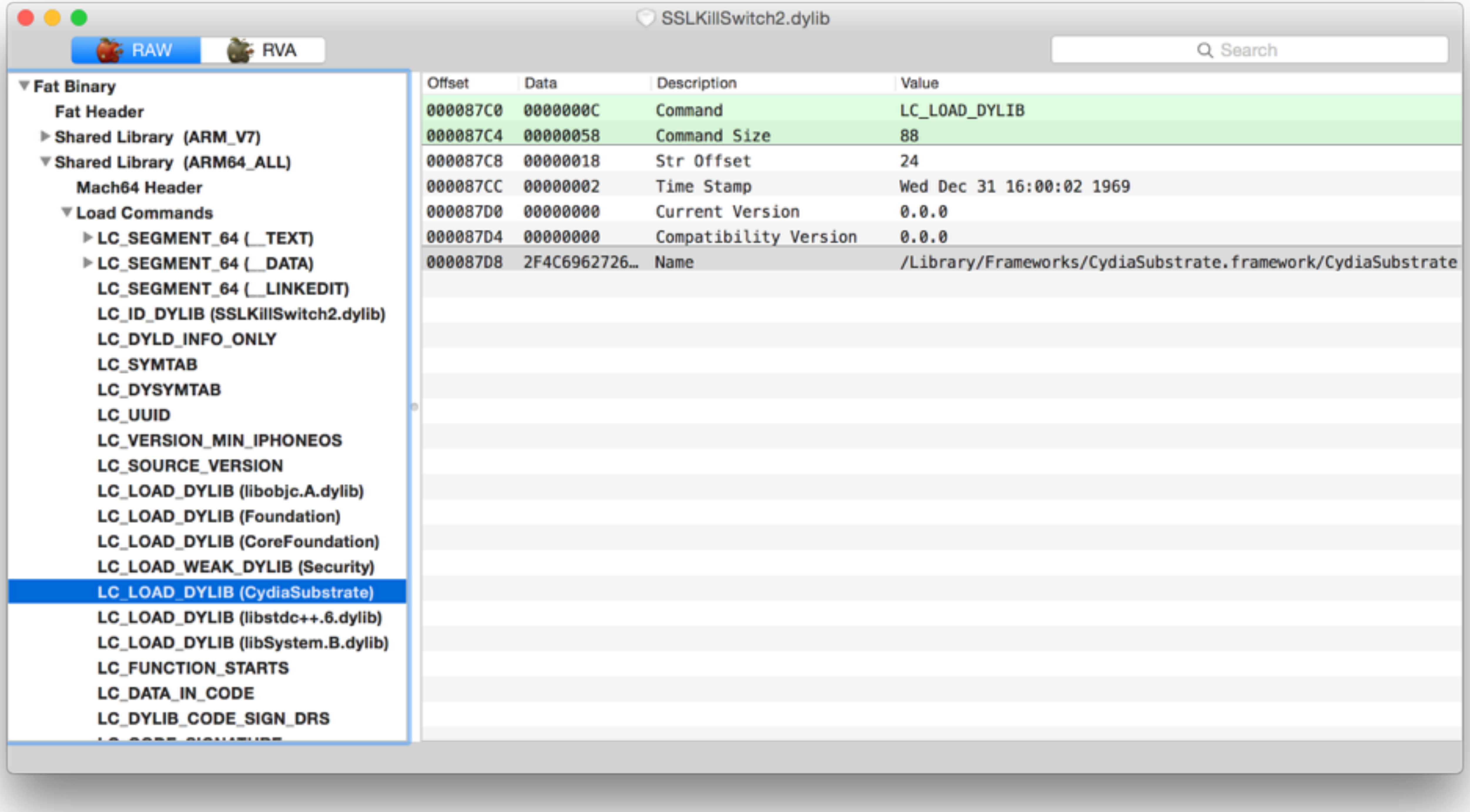
Substrate Tweaks



- Fat Binary
  - Fat Header
  - Shared Library (ARM_V7)
  - Shared Library (ARM64_ALL)
    - Mach64 Header
    - Load Commands
      - LC_SEGMENT_64 (__TEXT)
      - LC_SEGMENT_64 (__DATA)
      - LC_SEGMENT_64 (__LINKEDIT)
      - LC_ID_DYLIB (SSLKillSwitch2.dylib)
      - LC_DYLD_INFO_ONLY
      - LC_SYMTAB
      - LC_DYSYMTAB
      - LC_UUID
      - LC_VERSION_MIN_IPHONEOS
      - LC_SOURCE_VERSION
      - LC_LOAD_DYLIB (libobjc.A.dylib)
      - LC_LOAD_DYLIB (Foundation)
      - LC_LOAD_DYLIB (CoreFoundation)
      - LC_LOAD_WEAK_DYLIB (Security)
      - LC_LOAD_DYLIB (CydiaSubstrate)
      - LC_LOAD_DYLIB (libstdc++.6.dylib)
      - LC_LOAD_DYLIB (libSystem.B.dylib)
      - LC_FUNCTION_STARTS
      - LC_DATA_IN_CODE
      - LC_DYLIB_CODE_SIGN_DRS
      - LC_CODE_SIGNATURE

```
pFile     Data LO        Data HI                   Value
00008020  19 00 00 00…   5F 5F 54 45 58 54 00 00   ....(...__TEXT..
00008030  00 00 00 00…   00 00 00 00 00 00 00 00   ................
00008040  00 40 00 00…   00 00 00 00 00 00 00 00   .@..............
00008050  00 40 00 00…   05 00 00 00 05 00 00 00   .@..............
00008060  06 00 00 00…   5F 5F 74 65 78 74 00 00   ........__text..
00008070  00 00 00 00…   5F 5F 54 45 58 54 00 00   ........__TEXT..
00008080  00 00 00 00…   7C 3B 00 00 00 00 00 00   ........|;......
00008090  54 02 00 00…   7C 3B 00 00 02 00 00 00   T.......|;......
000080A0  00 00 00 00…   00 04 00 80 00 00 00 00   ................
000080B0  00 00 00 00…   5F 5F 73 74 75 62 73 00   ........__stubs.
000080C0  00 00 00 00…   5F 5F 54 45 58 54 00 00   ........__TEXT..
000080D0  00 00 00 00…   D0 3D 00 00 00 00 00 00   .........=......
000080E0  30 00 00 00…   D0 3D 00 00 01 00 00 00   0........=......
000080F0  00 00 00 00…   08 04 00 80 00 00 00 00   ................
00008100  0C 00 00 00…   5F 5F 73 74 75 62 5F 68   ........__stub_h
00008110  65 6C 70 65…   5F 5F 54 45 58 54 00 00   elper...__TEXT..
00008120  00 00 00 00…   00 3E 00 00 00 00 00 00   .........>......
00008130  48 00 00 00…   00 3E 00 00 02 00 00 00   H........>......
00008140  00 00 00 00…   00 04 00 80 00 00 00 00   ................
00008150  00 00 00 00…   5F 5F 63 73 74 72 69 6E   ........__cstrin
00008160  67 00 00 00…   5F 5F 54 45 58 54 00 00   g.......__TEXT..
00008170  00 00 00 00…   48 3E 00 00 00 00 00 00   ........H>......
00008180  F8 00 00 00…   48 3E 00 00 00 00 00 00   ........H>......
00008190  00 00 00 00…   02 00 00 00 00 00 00 00   ................
000081A0  00 00 00 00…   5F 5F 6F 62 6A 63 5F 6D   ........__objc_m
```

Substrate Tweaks



- Fat Binary
  - Fat Header
  - Shared Library (ARM_V7)
  - Shared Library (ARM64_ALL)
    - Mach64 Header
    - Load Commands
      - LC_SEGMENT_64 (__TEXT)
      - LC_SEGMENT_64 (__DATA)
      - LC_SEGMENT_64 (__LINKEDIT)
      - LC_ID_DYLIB (SSLKillSwitch2.dylib)
      - LC_DYLD_INFO_ONLY
      - LC_SYMTAB
      - LC_DYSYMTAB
      - LC_UUID
      - LC_VERSION_MIN_IPHONEOS
      - LC_SOURCE_VERSION
      - LC_LOAD_DYLIB (libobjc.A.dylib)
      - LC_LOAD_DYLIB (Foundation)
      - LC_LOAD_DYLIB (CoreFoundation)
      - LC_LOAD_WEAK_DYLIB (Security)
      - LC_LOAD_DYLIB (CydiaSubstrate)
      - LC_LOAD_DYLIB (libstdc++.6.dylib)
      - LC_LOAD_DYLIB (libSystem.B.dylib)
      - LC_FUNCTION_STARTS
      - LC_DATA_IN_CODE
      - LC_DYLIB_CODE_SIGN_DRS
      - LC_CODE_SIGNATURE

Offset	Data	Description	Value
000087C0	0000000C	Command	LC_LOAD_DYLIB
000087C4	00000058	Command Size	88
000087C8	00000018	Str Offset	24
000087CC	00000002	Time Stamp	Wed Dec 31 16:00:02 1969
000087D0	00000000	Current Version	0.0.0
000087D4	00000000	Compatibility Version	0.0.0
000087D8	2F4C6962726…	Name	/Library/Frameworks/CydiaSubstrate.framework/CydiaSubstrate

Substrate Tweaks

- What is a Substrate tweak again?
  - Dylib with a constructor to initialize hooks
  - CydiaSubstrate dylib as a dependency, for calling the hooking functions *MSHookFunction(), MSHookMessageEx()*

Substrate Tweaks

- What is a Substrate tweak again?
  - Dylib with a constructor to initialize hooks
  - CydiaSubstrate dylib as a dependency, for calling the hooking functions *MSHookFunction(), MSHookMessageEx()*
  - On a jailbroken device, gets auto-injected in running Apps

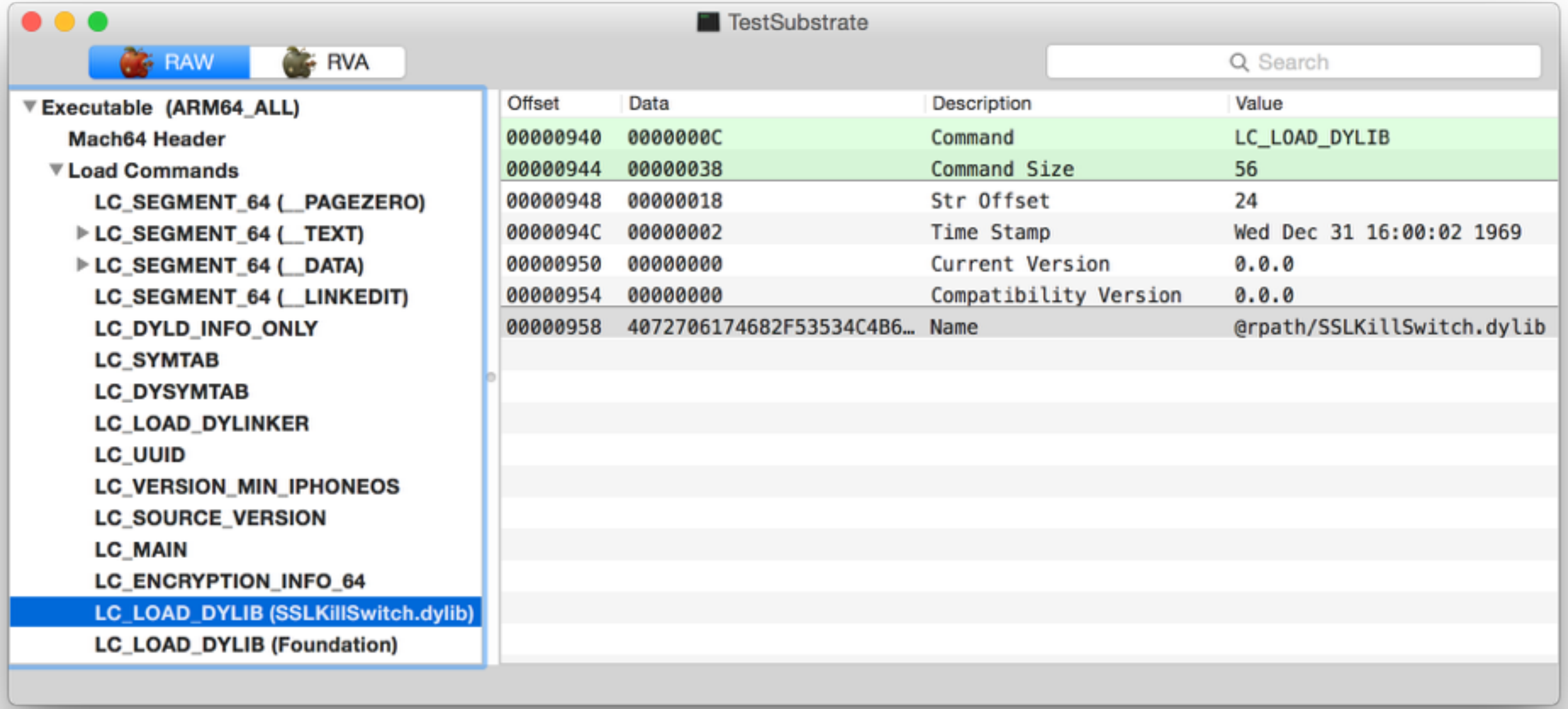
Substrate in an App

- Packaging ios-ssl-kill-switch in an App on a non-jailbroken device

Substrate in an App

- Packaging ios-ssl-kill-switch in an App on a non-jailbroken device
    - Put *SSLKillSwitch.dylib* in the App's bundle and add it as a dependency

Substrate in an App



- ▼ Executable (ARM64_ALL)
  - Mach64 Header
  - ▼ Load Commands
    - LC_SEGMENT_64 (__PAGEZERO)
    - ▶ LC_SEGMENT_64 (__TEXT)
    - ▶ LC_SEGMENT_64 (__DATA)
    - LC_SEGMENT_64 (__LINKEDIT)
    - LC_DYLD_INFO_ONLY
    - LC_SYMTAB
    - LC_DYSYMTAB
    - LC_LOAD_DYLINKER
    - LC_UUID
    - LC_VERSION_MIN_IPHONEOS
    - LC_SOURCE_VERSION
    - LC_MAIN
    - LC_ENCRYPTION_INFO_64
    - LC_LOAD_DYLIB (SSLKillSwitch.dylib)
    - LC_LOAD_DYLIB (Foundation)

Offset	Data	Description	Value
00000940	0000000C	Command	LC_LOAD_DYLIB
00000944	00000038	Command Size	56
00000948	00000018	Str Offset	24
0000094C	00000002	Time Stamp	Wed Dec 31 16:00:02 1969
00000950	00000000	Current Version	0.0.0
00000954	00000000	Compatibility Version	0.0.0
00000958	4072706174682F53534C4B6…	Name	@rpath/SSLKillSwitch.dylib

Substrate in an App

- Packaging ios-ssl-kill-switch in an App on a non-jailbroken device
  - Put *SSLKillSwitch.dylib* in the App's bundle and add it as a dependency

Substrate in an App

- Packaging ios-ssl-kill-switch in an App on a non-jailbroken device
    - Put *SSLKillSwitch.dylib* in the App's bundle and add it as a dependency
        - Dyld will then load the tweak when the App starts

Substrate in an App

```
Hardware Model:      iPhone6,1
Process:             TestSubstrate [319]
Path:                /private/var/mobile/Containers/Bundle/Application/D0D46AF8-2A3F-469D-
A30B-832E2AD2B459/TestSubstrate.nocodesigning.app/TestSubstrate
Identifier:          TestSubstrate
Version:             ???
Code Type:           ARM-64 (Native)
Parent Process:      launchd [1]
Date/Time:           2015-07-19 10:38:52.407 -0700
Launch Time:         2015-07-19 10:38:52.302 -0700
OS Version:          iOS 8.4 (12H143)
Report Version:      105
Exception Type:  EXC_BREAKPOINT (SIGTRAP)
Exception Codes: 0x0000000000000001, 0x00000001200c5088
Triggered by Thread:  0
Dyld Error Message:
  Library not loaded: @rpath/SSLKillSwitch.dylib
  Referenced from: /private/var/mobile/Containers/Bundle/Application/D0D46AF8-2A3F-469D-
A30B-832E2AD2B459/TestSubstrate.app/TestSubstrate
  Reason: no suitable image found.  Did find:
    /private/var/mobile/Containers/Bundle/Application/D0D46AF8-2A3F-469D-A30B-832E2AD2B459/
TestSubstrate.app/Frameworks/SSLKillSwitch.dylib: code signature invalid for '/private/var/
mobile/Containers/Bundle/Application/D0D46AF8-2A3F-469D-A30B-832E2AD2B459/TestSubstrate.app/
Frameworks/SSLKillSwitch.dylib'
```

Substrate in an App

```
Hardware Model:      iPhone6,1
Process:             TestSubstrate [319]
Path:                /private/var/mobile/Containers/Bundle/Application/D0D46AF8-2A3F-469D-
A30B-832E2AD2B459/TestSubstrate.nocodesigning.app/TestSubstrate
Identifier:          TestSubstrate
Version:             ???
Code Type:           ARM-64 (Native)
Parent Process:      launchd [1]
Date/Time:           2015-07-19 10:38:52.407 -0700
Launch Time:         2015-07-19 10:38:52.302 -0700
OS Version:          iOS 8.4 (12H143)
Report Version:      105
Exception Type:  EXC_BREAKPOINT (SIGTRAP)
Exception Codes: 0x0000000000000001, 0x00000001200c5088
Triggered by Thread:  0
Dyld Error Message:
  Library not loaded: @rpath/SSLKillSwitch.dylib
  Referenced from: /private/var/mobile/Containers/Bundle/Application/D0D46AF8-2A3F-469D-
A30B-832E2AD2B459/TestSubstrate.app/TestSubstrate
  Reason: no suitable image found.  Did find:
    /private/var/mobile/Containers/Bundle/Application/D0D46AF8-2A3F-469D-A30B-832E2AD2B459/
TestSubstrate.app/Frameworks/SSLKillSwitch.dylib: code signature invalid for '/private/var/
mobile/Containers/Bundle/Application/D0D46AF8-2A3F-469D-A30B-832E2AD2B459/TestSubstrate.app/
Frameworks/SSLKillSwitch.dylib'
```

Substrate in an App

```
Hardware Model:      iPhone6,1
Process:             TestSubstrate [319]
Path:                /private/var/mobile/Containers/Bundle/Application/D0D46AF8-2A3F-469D-
A30B-832E2AD2B459/TestSubstrate.nocodesigning.app/TestSubstrate
Identifier:          TestSubstrate
Version:             ???
Code Type:           ARM-64 (Native)
Parent Process:      launchd [1]
Date/Time:           2015-07-19 10:38:52.407 -0700
Launch Time:         2015-07-19 10:38:52.302 -0700
OS Version:          iOS 8.4 (12H143)
Report Version:      105
Exception Type:  EXC_BREAKPOINT (SIGTRAP)
Exception Codes: 0x0000000000000001, 0x00000001200c5088
Triggered by Thread:  0
Dyld Error Message:
  Library not loaded: @rpath/SSLKillSwitch.dylib
  Referenced from: /private/var/mobile/Containers/Bundle/Application/D0D46AF8-2A3F-469D-
A30B-832E2AD2B459/TestSubstrate.app/TestSubstrate
  Reason: no suitable image found.  Did find:
    /private/var/mobile/Containers/Bundle/Application/D0D46AF8-2A3F-469D-A30B-832E2AD2B459/
TestSubstrate.app/Frameworks/SSLKillSwitch.dylib: code signature invalid for '/private/var/
mobile/Containers/Bundle/Application/D0D46AF8-2A3F-469D-A30B-832E2AD2B459/TestSubstrate.app/
Frameworks/SSLKillSwitch.dylib'
```

Substrate in an App

```
Hardware Model:      iPhone6,1
Process:             TestSubstrate [319]
Path:                /private/var/mobile/Containers/Bundle/Application/D0D46AF8-2A3F-469D-
A30B-832E2AD2B459/TestSubstrate.nocodesigning.app/TestSubstrate
Identifier:          TestSubstrate
Version:             ???
Code Type:           ARM-64 (Native)
Parent Process:      launchd [1]
Date/Time:           2015-07-19 10:38:52.407 -0700
Launch Time:         2015-07-19 10:38:52.302 -0700
OS Version:          iOS 8.4 (12H143)
Report Version:      105
Exception Type:  EXC_BREAKPOINT (SIGTRAP)
Exception Codes: 0x0000000000000001, 0x00000001200c5088
Triggered by Thread:  0
Dyld Error Message:
  Library not loaded: @rpath/SSLKillSwitch.dylib
  Referenced from: /private/var/mobile/Containers/Bundle/Application/D0D46AF8-2A3F-469D-
A30B-832E2AD2B459/TestSubstrate.app/TestSubstrate
  Reason: no suitable image found.  Did find:
    /private/var/mobile/Containers/Bundle/Application/D0D46AF8-2A3F-469D-A30B-832E2AD2B459/
TestSubstrate.app/Frameworks/SSLKillSwitch.dylib: code signature invalid for '/private/var/
mobile/Containers/Bundle/Application/D0D46AF8-2A3F-469D-A30B-832E2AD2B459/TestSubstrate.app/
Frameworks/SSLKillSwitch.dylib'
```

Substrate in an App

- Packaging ios-ssl-kill-switch in an App on a non-jailbroken device
    - Put *SSLKillSwitch.dylib* in the App's bundle and add it as a dependency
        - Dyld will then load the tweak when the App starts

Substrate in an App

- Packaging ios-ssl-kill-switch in an App on a non-jailbroken device
  - Put *SSLKillSwitch.dylib* in the App's bundle and add it as a dependency
    - Dyld will then load the tweak when the App starts
    - And also code-sign the tweak…

Substrate in an App

```
Hardware Model:      iPhone6,1
Process:             TestSubstrate [311]
Path:                /private/var/mobile/Containers/Bundle/Application/
3EFA0205-4971-46B6-A1A3-77D3AA6793F5/TestSubstrate.nocydia.app/TestSubstrate
Identifier:          TestSubstrate
Version:             ???
Code Type:           ARM-64 (Native)
Parent Process:      launchd [1]
Date/Time:           2015-07-19 10:31:18.880 -0700
Launch Time:         2015-07-19 10:31:18.734 -0700
OS Version:          iOS 8.4 (12H143)
Report Version:      105
Exception Type:  EXC_BREAKPOINT (SIGTRAP)
Exception Codes: 0x0000000000000001, 0x0000000120001088
Triggered by Thread:  0
Dyld Error Message:
  Library not loaded: /Library/Frameworks/CydiaSubstrate.framework/CydiaSubstrate
  Referenced from: /private/var/mobile/Containers/Bundle/Application/
3EFA0205-4971-46B6-A1A3-77D3AA6793F5/TestSubstrate.app/Frameworks/
SSLKillSwitch.dylib
  Reason: image not found
```

Substrate in an App

```
Hardware Model:      iPhone6,1
Process:             TestSubstrate [311]
Path:                /private/var/mobile/Containers/Bundle/Application/
3EFA0205-4971-46B6-A1A3-77D3AA6793F5/TestSubstrate.nocydia.app/TestSubstrate
Identifier:          TestSubstrate
Version:             ???
Code Type:           ARM-64 (Native)
Parent Process:      launchd [1]
Date/Time:           2015-07-19 10:31:18.880 -0700
Launch Time:         2015-07-19 10:31:18.734 -0700
OS Version:          iOS 8.4 (12H143)
Report Version:      105
Exception Type:  EXC_BREAKPOINT (SIGTRAP)
Exception Codes: 0x0000000000000001, 0x0000000120001088
Triggered by Thread:  0
Dyld Error Message:
  Library not loaded: /Library/Frameworks/CydiaSubstrate.framework/CydiaSubstrate
  Referenced from: /private/var/mobile/Containers/Bundle/Application/
3EFA0205-4971-46B6-A1A3-77D3AA6793F5/TestSubstrate.app/Frameworks/
SSLKillSwitch.dylib
  Reason: image not found
```

Substrate in an App

```
Hardware Model:      iPhone6,1
Process:             TestSubstrate [311]
Path:                /private/var/mobile/Containers/Bundle/Application/
3EFA0205-4971-46B6-A1A3-77D3AA6793F5/TestSubstrate.nocydia.app/TestSubstrate
Identifier:          TestSubstrate
Version:             ???
Code Type:           ARM-64 (Native)
Parent Process:      launchd [1]
Date/Time:           2015-07-19 10:31:18.880 -0700
Launch Time:         2015-07-19 10:31:18.734 -0700
OS Version:          iOS 8.4 (12H143)
Report Version:      105
Exception Type:  EXC_BREAKPOINT (SIGTRAP)
Exception Codes: 0x0000000000000001, 0x0000000120001088
Triggered by Thread:  0
Dyld Error Message:
  Library not loaded: /Library/Frameworks/CydiaSubstrate.framework/CydiaSubstrate
  Referenced from: /private/var/mobile/Containers/Bundle/Application/
3EFA0205-4971-46B6-A1A3-77D3AA6793F5/TestSubstrate.app/Frameworks/
SSLKillSwitch.dylib
  Reason: image not found
```

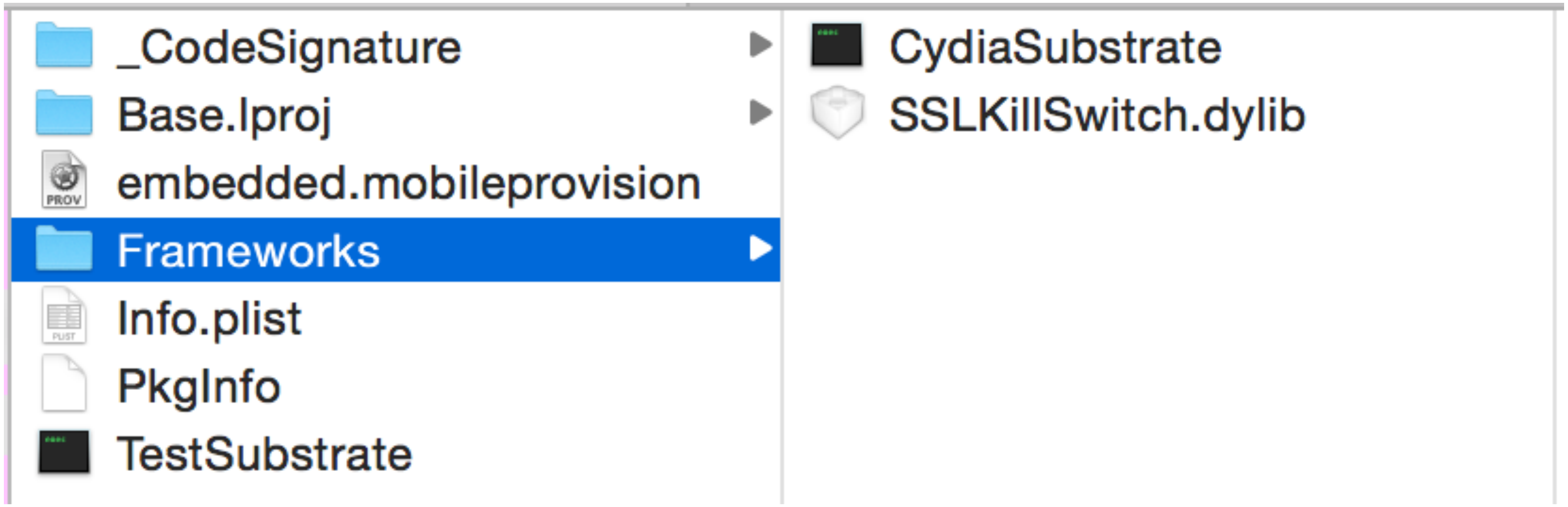
Substrate in an App

- Packaging ios-ssl-kill-switch in an App on a non-jailbroken device
    - Put *SSLKillSwitch.dylib* in the App’s bundle and add it as a dependency
        - Dyld will then load the tweak when the App starts
        - And also code-sign the tweak…

Substrate in an App

- Packaging ios-ssl-kill-switch in an App on a non-jailbroken device
    - Put *SSLKillSwitch.dylib* in the App's bundle and add it as a dependency
        - Dyld will then load the tweak when the App starts
        - And also code-sign the tweak…
    - Also embed CydiaSubstrate in the App's bundle
        - Rewrite the path to CydiaSubstrate within the tweak's *LC_LOAD_DYLIB* load commands

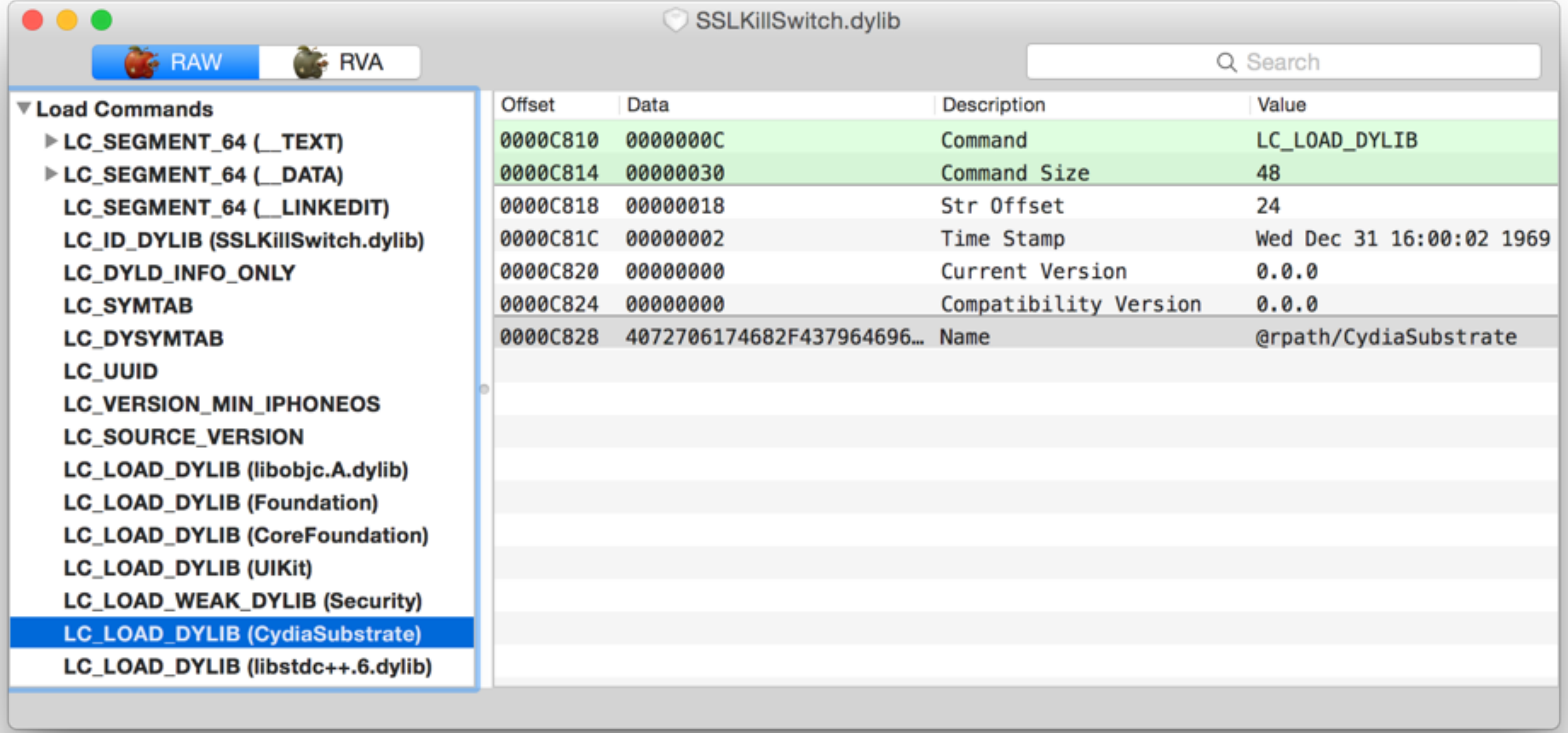
Substrate in an App

- 

_CodeSignature
Base.lproj
embedded.mobileprovision
Frameworks
Info.plist
PkgInfo
TestSubstrate

CydiaSubstrate
SSLKillSwitch.dylib

Substrate in an App



SSLKillSwitch.dylib

- Load Commands
  - LC_SEGMENT_64 (__TEXT)
  - LC_SEGMENT_64 (__DATA)
  - LC_SEGMENT_64 (__LINKEDIT)
  - LC_ID_DYLIB (SSLKillSwitch.dylib)
  - LC_DYLD_INFO_ONLY
  - LC_SYMTAB
  - LC_DYSYMTAB
  - LC_UUID
  - LC_VERSION_MIN_IPHONEOS
  - LC_SOURCE_VERSION
  - LC_LOAD_DYLIB (libobjc.A.dylib)
  - LC_LOAD_DYLIB (Foundation)
  - LC_LOAD_DYLIB (CoreFoundation)
  - LC_LOAD_DYLIB (UIKit)
  - LC_LOAD_WEAK_DYLIB (Security)
  - LC_LOAD_DYLIB (CydiaSubstrate)
  - LC_LOAD_DYLIB (libstdc++.6.dylib)

Offset	Data	Description	Value
0000C810	0000000C	Command	LC_LOAD_DYLIB
0000C814	00000030	Command Size	48
0000C818	00000018	Str Offset	24
0000C81C	00000002	Time Stamp	Wed Dec 31 16:00:02 1969
0000C820	00000000	Current Version	0.0.0
0000C824	00000000	Compatibility Version	0.0.0
0000C828	4072706174682F437964696…	Name	@rpath/CydiaSubstrate

Substrate in an App

```
Hardware Model:      iPhone6,1
Process:             TestSubstrate [1438]
Path:                /private/var/mobile/Containers/Bundle/Application/AF0E2FD7-
BA47-4E57-95ED-B2C3D6116E62/TestSubstrate.app/TestSubstrate
Identifier:          TestSubstrate
Version:             ???
Code Type:           ARM-64 (Native)
Parent Process:      launchd [1]
Date/Time:           2015-07-16 22:57:43.529 -0700
Launch Time:         2015-07-16 22:57:43.356 -0700
OS Version:          iOS 8.4 (12H143)
Report Version:      105
Exception Type:  EXC_BAD_ACCESS (SIGKILL - CODESIGNING)
Exception Subtype: unknown at 0x0000000186b346c4
Triggered by Thread:  0
Thread 0 name:  Dispatch queue: com.apple.main-thread
Thread 0 Crashed:
0   CydiaSubstrate                   0x00000001000931bc 0x100090000 + 12732
1   SSLKillSwitch.dylib              0x0000000100087d30 0x100084000 + 15664
2   dyld                             0x000000012006d234 0x12005c000 + 70196
3   dyld                             0x000000012006d3ec 0x12005c000 + 70636
[...]
```

Substrate in an App

```
Hardware Model:      iPhone6,1
Process:             TestSubstrate [1438]
Path:                /private/var/mobile/Containers/Bundle/Application/AF0E2FD7-
BA47-4E57-95ED-B2C3D6116E62/TestSubstrate.app/TestSubstrate
Identifier:          TestSubstrate
Version:             ???
Code Type:           ARM-64 (Native)
Parent Process:      launchd [1]
Date/Time:           2015-07-16 22:57:43.529 -0700
Launch Time:         2015-07-16 22:57:43.356 -0700
OS Version:          iOS 8.4 (12H143)
Report Version:      105
Exception Type:  EXC_BAD_ACCESS (SIGKILL - CODESIGNING)
Exception Subtype: unknown at 0x0000000186b346c4
Triggered by Thread:  0
Thread 0 name:  Dispatch queue: com.apple.main-thread
Thread 0 Crashed:
0   CydiaSubstrate                    0x00000001000931bc 0x100090000 + 12732
1   SSLKillSwitch.dylib               0x0000000100087d30 0x100084000 + 15664
2   dyld                              0x000000012006d234 0x12005c000 + 70196
3   dyld                              0x000000012006d3ec 0x12005c000 + 70636
[...]
```

Substrate in an App

```
Hardware Model:      iPhone6,1
Process:             TestSubstrate [1438]
Path:                /private/var/mobile/Containers/Bundle/Application/AF0E2FD7-
BA47-4E57-95ED-B2C3D6116E62/TestSubstrate.app/TestSubstrate
Identifier:          TestSubstrate
Version:             ???
Code Type:           ARM-64 (Native)
Parent Process:      launchd [1]
Date/Time:           2015-07-16 22:57:43.529 -0700
Launch Time:         2015-07-16 22:57:43.356 -0700
OS Version:          iOS 8.4 (12H143)
Report Version:      105
Exception Type:  EXC_BAD_ACCESS (SIGKILL - CODESIGNING)
Exception Subtype: unknown at 0x0000000186b346c4
Triggered by Thread:  0
Thread 0 name:  Dispatch queue: com.apple.main-thread
Thread 0 Crashed:
0   CydiaSubstrate                    0x00000001000931bc 0x100090000 + 12732
1   SSLKillSwitch.dylib               0x0000000100087d30 0x100084000 + 15664
2   dyld                              0x000000012006d234 0x12005c000 + 70196
3   dyld                              0x000000012006d3ec 0x12005c000 + 70636
[...]
```

Substrate in an App

```
Hardware Model:      iPhone6,1
Process:             TestSubstrate [1438]
Path:                /private/var/mobile/Containers/Bundle/Application/AF0E2FD7-
BA47-4E57-95ED-B2C3D6116E62/TestSubstrate.app/TestSubstrate
Identifier:          TestSubstrate
Version:             ???
Code Type:           ARM-64 (Native)
Parent Process:      launchd [1]
Date/Time:           2015-07-16 22:57:43.529 -0700
Launch Time:         2015-07-16 22:57:43.356 -0700
OS Version:          iOS 8.4 (12H143)
Report Version:      105
Exception Type:  EXC_BAD_ACCESS (SIGKILL - CODESIGNING)
Exception Subtype: unknown at 0x0000000186b346c4
Triggered by Thread:  0
Thread 0 name:  Dispatch queue: com.apple.main-thread
Thread 0 Crashed:
0   CydiaSubstrate                0x00000001000931bc 0x100090000 + 12732 MSFunctionHook()
1   SSLKillSwitch.dylib           0x0000000100087d30 0x100084000 + 15664 Dylib Contructor
2   dyld                          0x000000012006d234 0x12005c000 + 70196
3   dyld                          0x000000012006d3ec 0x12005c000 + 70636
[...]
```

Substrate in an App

- SIGKILL when calling *MSFunctionHook()*
    - Substrate hooks C functions by patching the function's prologue
    - This requires RWX memory pages
        - Not possible on a non-jailbroken device…

Substrate in an App

- SIGKILL when calling *MSFunctionHook()*
  - Substrate hooks C functions by patching the function's prologue
  - This requires RWX memory pages
    - Not possible on a non-jailbroken device…
    - …Unless running in a debugger

Substrate in an App

- We failed :(
  - No way to package a Substrate tweak in an App Store App due to RWX requirement

Substrate in an App

- We failed :(
  - No way to package a Substrate tweak in an App Store App due to RWX requirement
- Initial goal was to hook functions and patch an App at runtime on a non-jailbroken device
  - Any alternatives?

Hooking Jailbreak-Free

- Other other hooking techniques on iOS
  - DYLID_INSERT_LIBRARIES and __interpose
    - Symbol rebinding: can only “hook" exported functions

Hooking Jailbreak-Free

- Other other hooking techniques on iOS

```
// Structure for interposing functions
typedef struct interpose_s {
    void *new_func;
    void *orig_func; } interpose_t;

// Our replacement functions
void *my_malloc(int size);
void my_free (void *);

// Add the interpose section
static const interpose_t interposing_functions[] \
__attribute__ ((section("__DATA, __interpose"))) = {
    { (void *)my_free, (void *)free },
    { (void *)my_malloc, (void *)malloc }
};
```

Hooking Jailbreak-Free

- Other other hooking techniques on iOS
    - DYLID_INSERT_LIBRARIES and __interpose
        - Symbol rebinding: can only “hook" exported functions

Hooking Jailbreak-Free

- Other other hooking techniques on iOS
  - DYLID_INSERT_LIBRARIES and __interpose
    - Symbol rebinding: can only “hook" exported functions
    - Requires setting an environment variable
      - Can’t be done in an App Store App outside of Xcode

Hooking Jailbreak-Free

- Other other hooking techniques on iOS
  - Newer libraries for dynamic symbol rebinding
    - facebook/fishhook
    - comex/substitute
      - Specifically *substitute_interpose_imports()*
      - Also supports hooking via function prologue patching (like Substrate) if RWX available

Agenda

- Dynamic Libraries and iOS 8
- Cydia Substrate on a Non-Jailbroken Device
- Putting It All Together: TrustKit

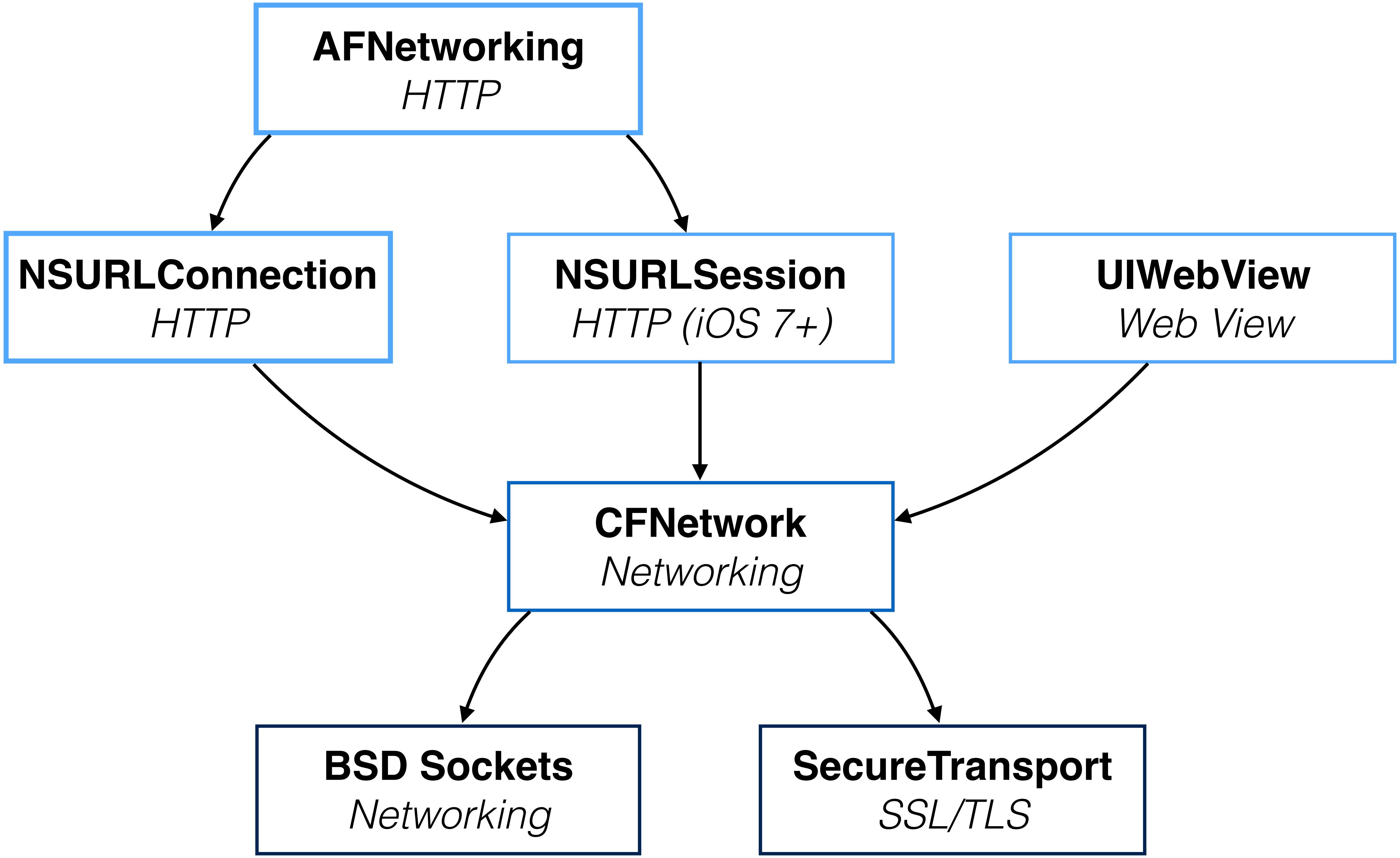
Agenda

- Dynamic Libraries and iOS 8
- Cydia Substrate on a Non-Jailbroken Device
- Putting It All Together: TrustKit

TrustKit

- Effortless SSL pinning for iOS and OS X
- “Tweak" / runtime patch targeting SecureTransport
  - Uses *facebook/fishhook* for C function hooking

iOS Network Stack



AFNetworking
HTTP

NSURLConnection
HTTP

NSURLSession
HTTP (iOS 7+)

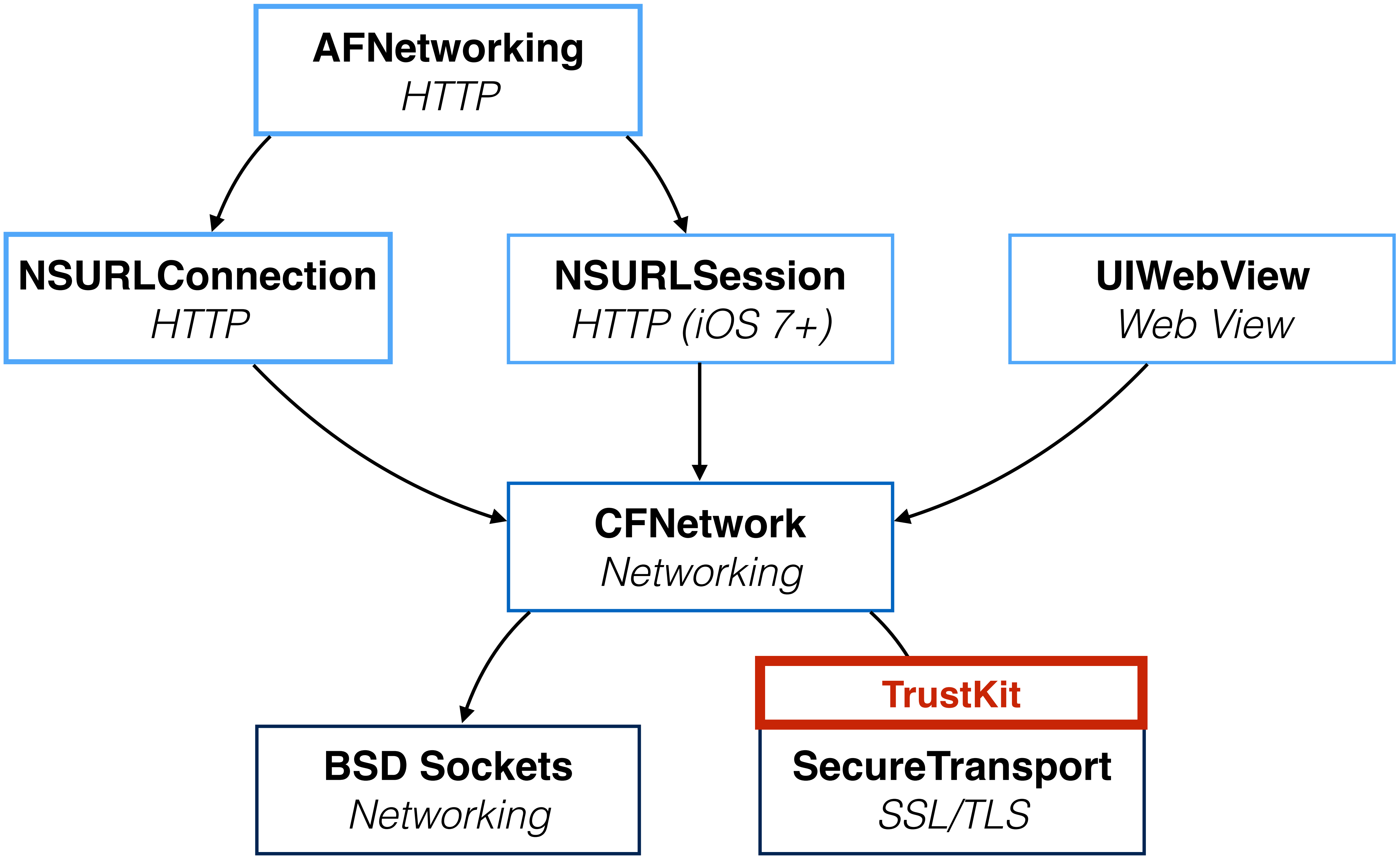
UIWebView
Web View

CFNetwork
Networking

BSD Sockets
Networking

SecureTransport
SSL/TLS

iOS Network Stack



AFNetworking
HTTP

NSURLConnection
HTTP

NSURLSession
HTTP (iOS 7+)

UIWebView
Web View

CFNetwork
Networking

BSD Sockets
Networking

TrustKit

SecureTransport
SSL/TLS

TrustKit

- Effortless SSL pinning for iOS and OS X
- “Tweak" / runtime patch targeting SecureTransport
    - Uses *facebook/fishhook* for C function hooking

TrustKit

- Effortless SSL pinning for iOS and OS X
- “Tweak" / runtime patch targeting SecureTransport
  - Uses *facebook/fishhook* for C function hooking
- Drag & Drop in Xcode
  - Can be deployed without changing the App’s source code

TrustKit

- Effortless SSL pinning for iOS and OS X
- “Tweak" / runtime patch targeting SecureTransport
    - Uses *facebook/fishhook* for C function hooking
- Drag & Drop in Xcode
    - Can be deployed without changing the App’s source code
- Needed a usable solution that **works in real-world Apps**
    - Collaborated with the Yahoo mobile & security teams

SSL Pinning at Yahoo

- Goal: SSL pinning for Yahoo’s mobile Apps
    - Easy project, right?

SSL Pinning at Yahoo

- Goal: SSL pinning for Yahoo’s mobile Apps
  - Easy project, right?
- But...
  - Technical challenges: What and how to pin?
  - Operational challenges: How to get buy-in from management?

Technical Challenges

- What to pin?
  - Certificate or public key?
    - Best practice is Subject Public Key Info
      - No API on iOS to extract SPKI from a certificate…
- Most libraries and examples are doing it wrong
  - Comparing the whole certificate or public key

Technical Challenges

- How to pin?
  - Find and modify every single instance of *NSURLConnection*, *NSURLSession* ?
    - Or better: use method swizzling
  - Problem: no public API for customizing certificate validation in UIWebView
    - Not even swizzling would work

Operational Challenges

- How to get buy-in from management?
  - Blocking attackers is a good cause but...

Operational Challenges

- How to get buy-in from management?
    - Blocking attackers is a good cause but...
        - What if we block the wrong connections?

Operational Challenges

- How to get buy-in from management?
  - Blocking attackers is a good cause but...
    - What if we block the wrong connections?
- Answer: a **report-only** mode
  - Shows what connections would be blocked and why
  - Easier to decide on whether pinning should be enforced or not

SSL Pinning at Yahoo

- No existing iOS library supported **any** of these requirements
    - SPKI pinning
    - Report-only mode
    - Easy to deploy but works on all networking APIs
- Met with Data Theorem and started a collaboration :)

TrustKit

- We solved these challenges
  - SPKI pinning: ask the developer what the key's algorithm is
  - Easy configuration
    - Heavily based on HTTP Public Key Pinning
  - Works on all Apple APIs
  - Report-only mode
    - Format similar to HPKP for pin failure reports

Demo

TrustKit

- We’re open-sourcing TrustKit today
    - Supports iOS 7+ and OS X10.9+
    - MIT license
    - Will also be available via CocoaPods very soon
- https://datatheorem.github.io/TrustKit/
    - Feedback, comments and pull requests very welcome!

Conclusion

- TrustKit is already live in a Yahoo App on the App Store
    - Partnered with other companies who will deploy it in their OS X and iOS Apps
- Used our experience in offense to build a defensive library
    - Code injection, function hooking
    - Could be applied to other things than SSL pinning?

One Last Thing

- SSL pinning can be a challenge for security researchers
  - And is not designed to block an attacker running code as root on the device…
  - So I also just released SSL Kill Switch 2
    - https://github.com/nabla-c0d3/ssl-kill-switch2
    - Added support for TrustKit Apps (and OS X)

Thanks!