Trusting SDKs

Felix Krause <felix@krausefx.com>

@KrauseFx

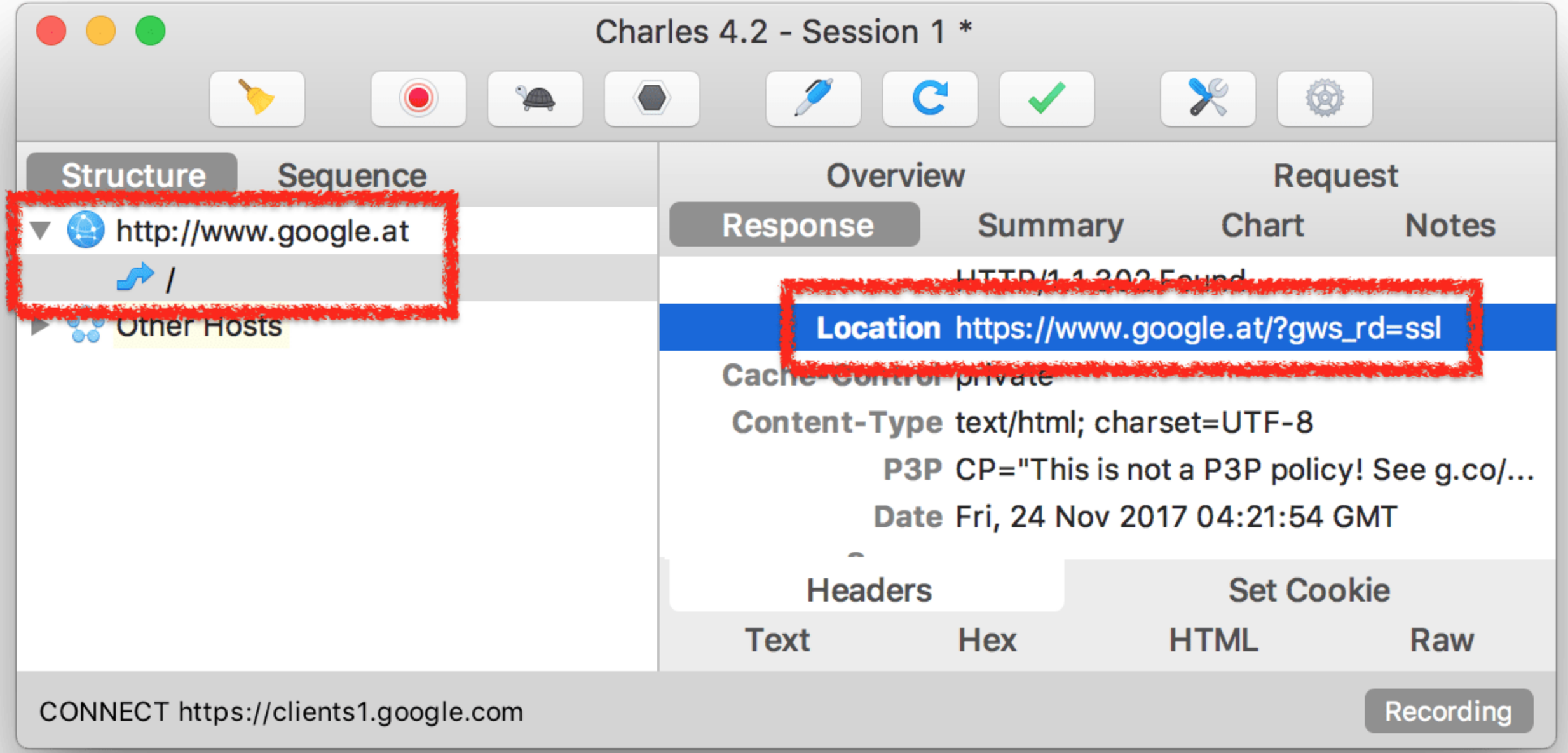
31% of the top SDKs affected

Worst case?

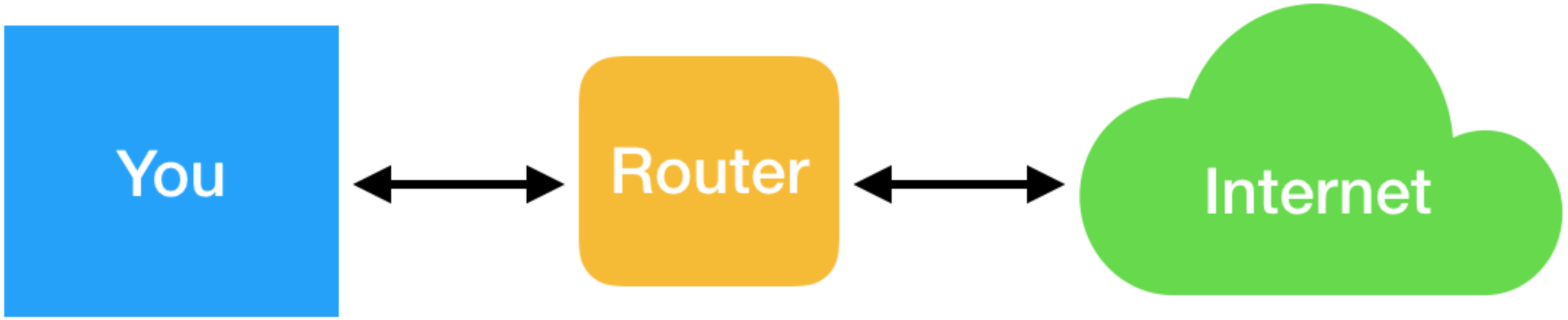
Web Security 101

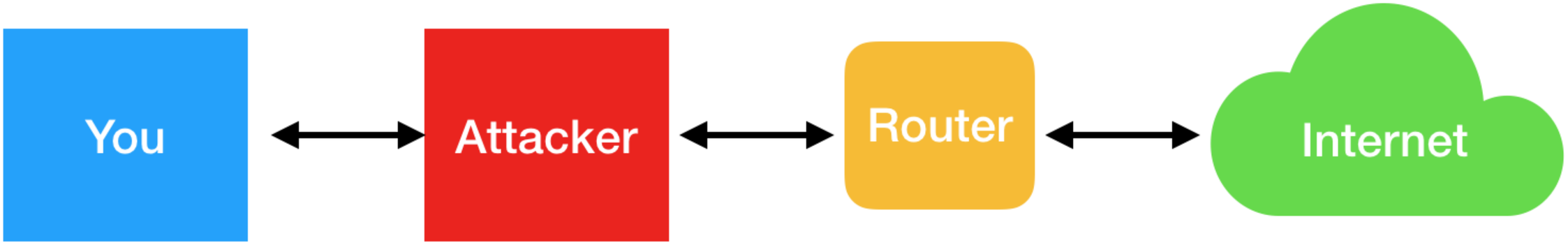
HTTP

HTTPS

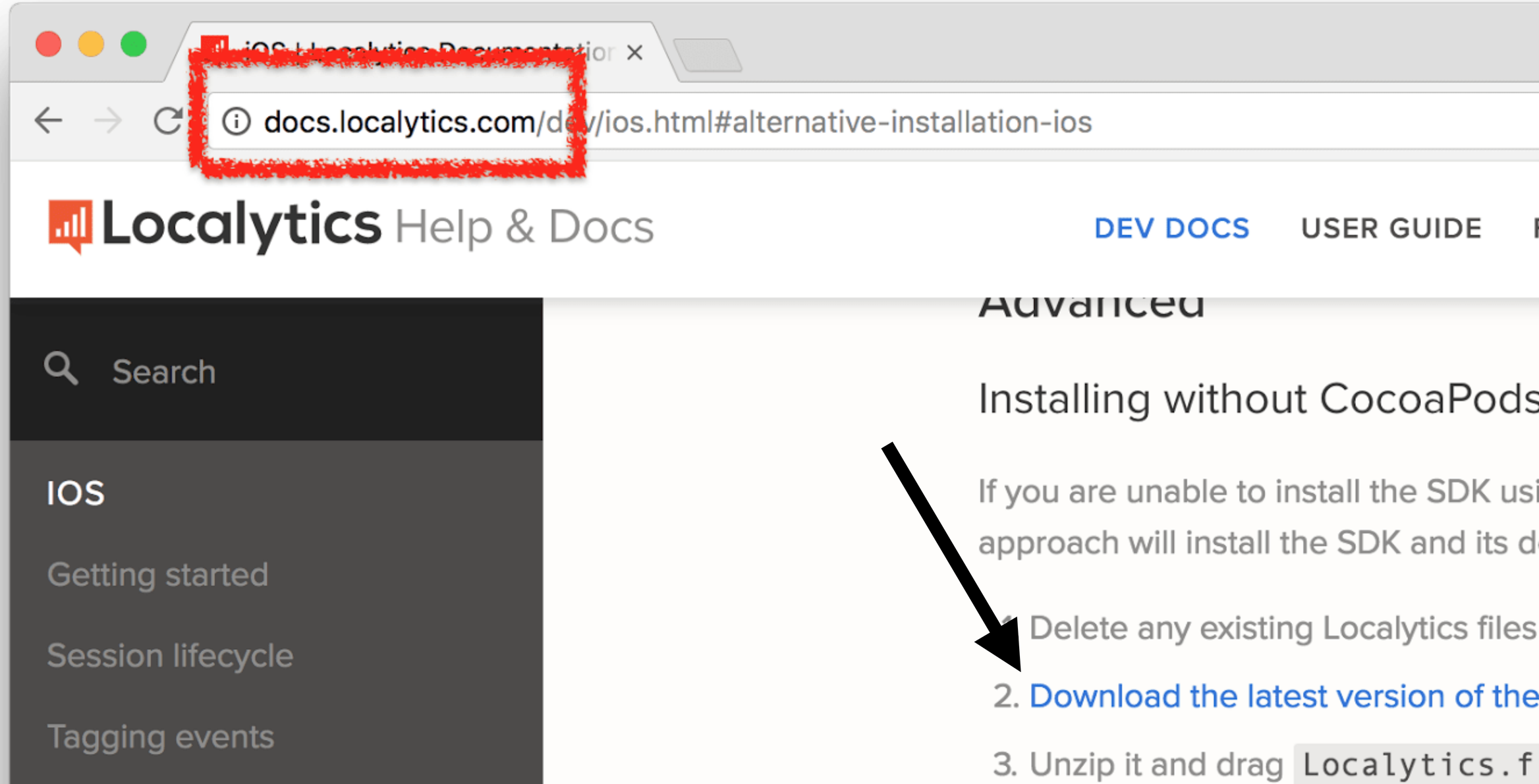

Charles 4.2 - Session 1 *
Structure
Sequence
http://www.google.at
/
Other Hosts
Overview
Request
Response
Summary
Chart
Notes
Location https://www.google.at/?gws_rd=ssl
Content-Type text/html; charset=UTF-8
P3P CP="This is not a P3P policy! See g.co/...
Date Fri, 24 Nov 2017 04:21:54 GMT
Headers
Set Cookie
Text
Hex
HTML
Raw
CONNECT https://clients1.google.com
Recording

Obligatory OSI layer diagram


You
Router
Internet

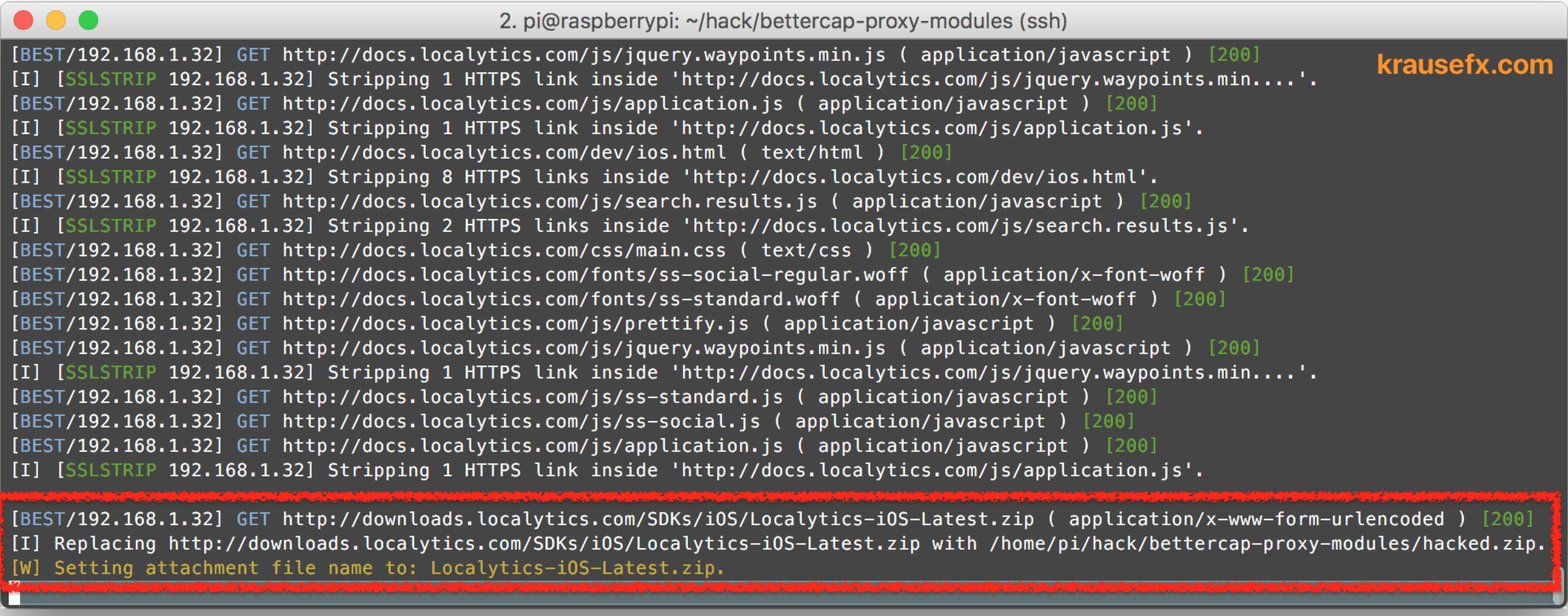

You
Attacker
Router
Internet

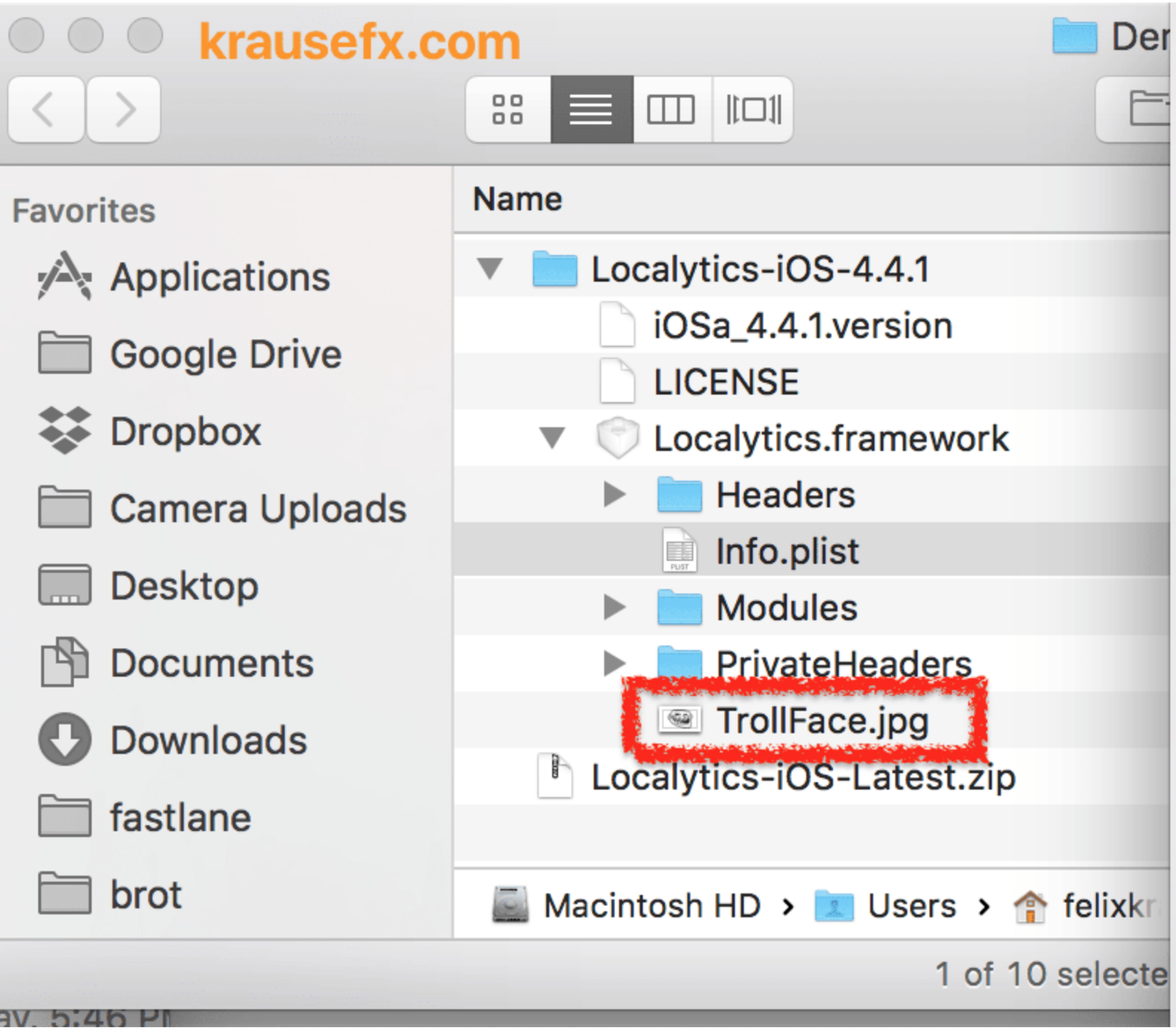
CocoaPods


docs.localytics.com/dev/ios.html#alternative-installation-ios
Localytics Help & Docs
DEV DOCS
USER GUIDE
Search
IOS
Getting started
Session lifecycle
Tagging events
Advanced
Installing without CocoaPods
If you are unable to install the SDK usi
approach will install the SDK and its d
1. Delete any existing Localytics files
2. Download the latest version of the
3. Unzip it and drag Localytics.f

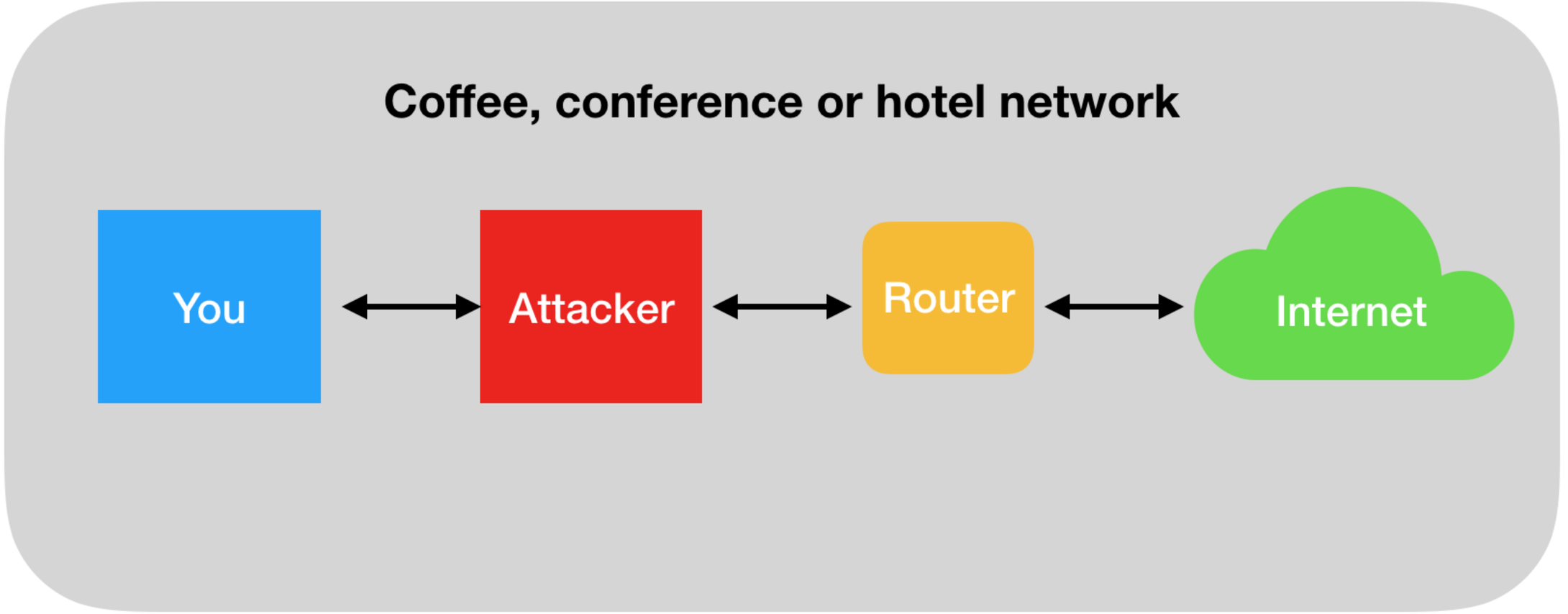
https://s3.aws.com/localytics-sdks/sdk.zip

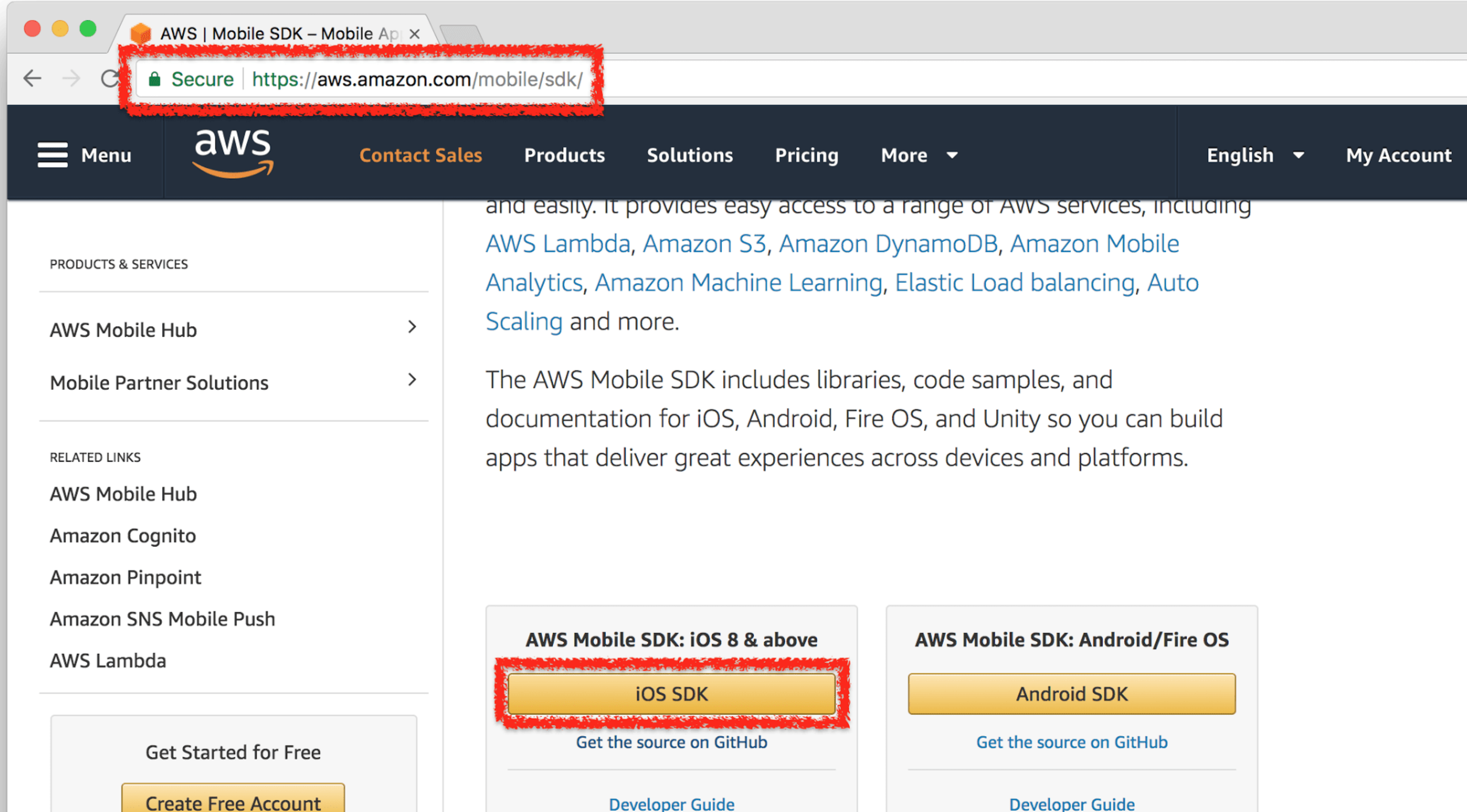
https://s3.aws.com/localytics-binaries/sdk.zip

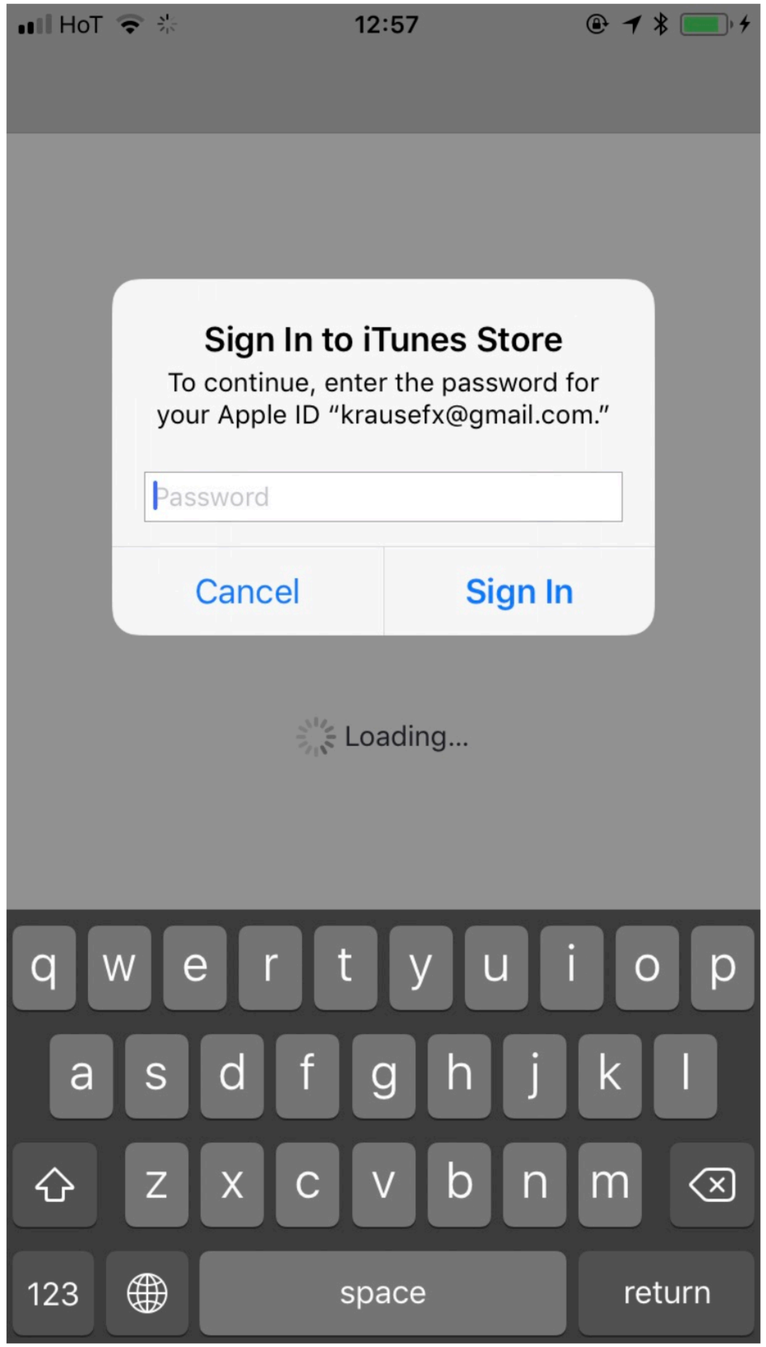
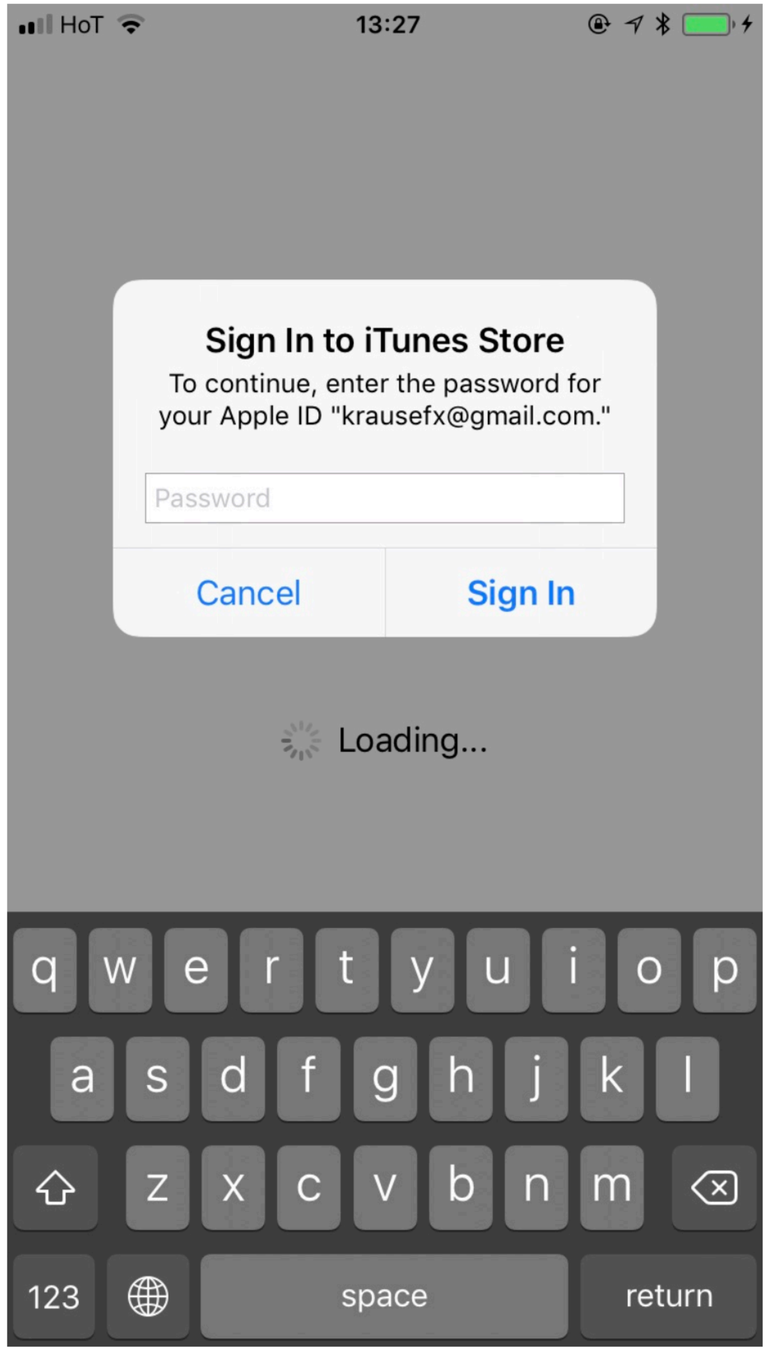

2. pi@raspberrypi: ~/hack/bettercap-proxy-modules (ssh)
[BEST/192.168.1.32] GET http://docs.localytics.com/js/jquery.waypoints.min.js (application/javascript) [200]
[I] [SSLSTRIP 192.168.1.32] Stripping 1 HTTPS link inside 'http://docs.localytics.com/js/jquery.waypoints.min....'.
[BEST/192.168.1.32] GET http://docs.localytics.com/js/application.js (application/javascript) [200]
[I] [SSLSTRIP 192.168.1.32] Stripping 1 HTTPS link inside 'http://docs.localytics.com/js/application.js'.
[BEST/192.168.1.32] GET http://docs.localytics.com/dev/ios.html (text/html) [200]
[I] [SSLSTRIP 192.168.1.32] Stripping 8 HTTPS links inside 'http://docs.localytics.com/dev/ios.html'.
[BEST/192.168.1.32] GET http://docs.localytics.com/js/search.results.js (application/javascript) [200]
[I] [SSLSTRIP 192.168.1.32] Stripping 2 HTTPS links inside 'http://docs.localytics.com/js/search.results.js'.
[BEST/192.168.1.32] GET http://docs.localytics.com/css/main.css (text/css) [200]
[BEST/192.168.1.32] GET http://docs.localytics.com/fonts/ss-social-regular.woff (application/x-font-woff) [200]
[BEST/192.168.1.32] GET http://docs.localytics.com/fonts/ss-standard.woff (application/x-font-woff) [200]
[BEST/192.168.1.32] GET http://docs.localytics.com/js/prettify.js (application/javascript) [200]
[BEST/192.168.1.32] GET http://docs.localytics.com/js/jquery.waypoints.min.js (application/javascript) [200]
[I] [SSLSTRIP 192.168.1.32] Stripping 1 HTTPS link inside 'http://docs.localytics.com/js/jquery.waypoints.min....'.
[BEST/192.168.1.32] GET http://docs.localytics.com/js/ss-standard.js (application/javascript) [200]
[BEST/192.168.1.32] GET http://docs.localytics.com/js/ss-social.js (application/javascript) [200]
[BEST/192.168.1.32] GET http://docs.localytics.com/js/application.js (application/javascript) [200]
[I] [SSLSTRIP 192.168.1.32] Stripping 1 HTTPS link inside 'http://docs.localytics.com/js/application.js'.
[BEST/192.168.1.32] GET http://downloads.localytics.com/SDKs/iOS/Localytics-iOS-Latest.zip (application/x-www-form-urlencoded) [200]
[I] Replacing http://downloads.localytics.com/SDKs/iOS/Localytics-iOS-Latest.zip with /home/pi/hack/bettercap-proxy-modules/hacked.zip.
[W] Setting attachment file name to: Localytics-iOS-Latest.zip.
krausefx.com

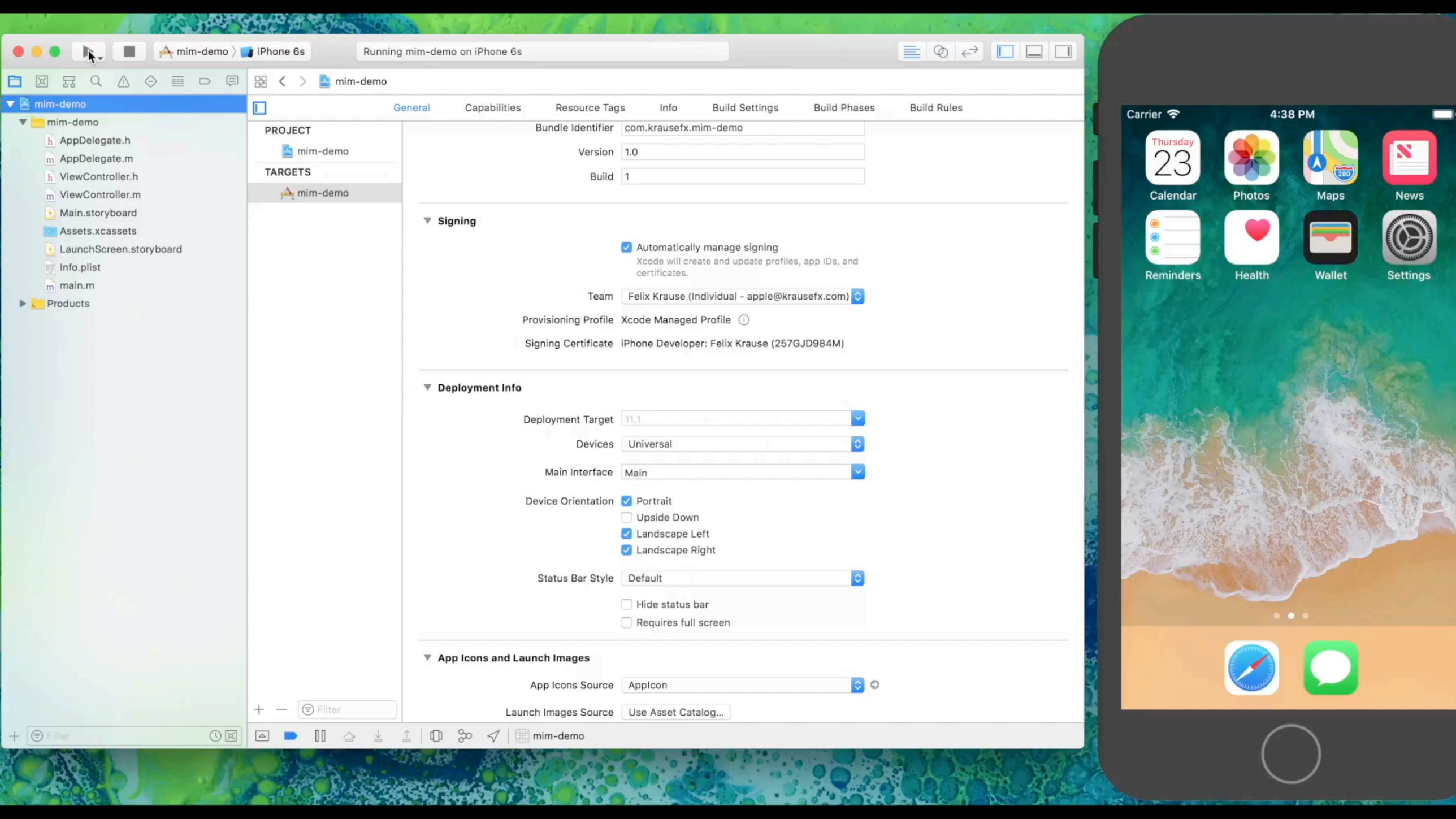


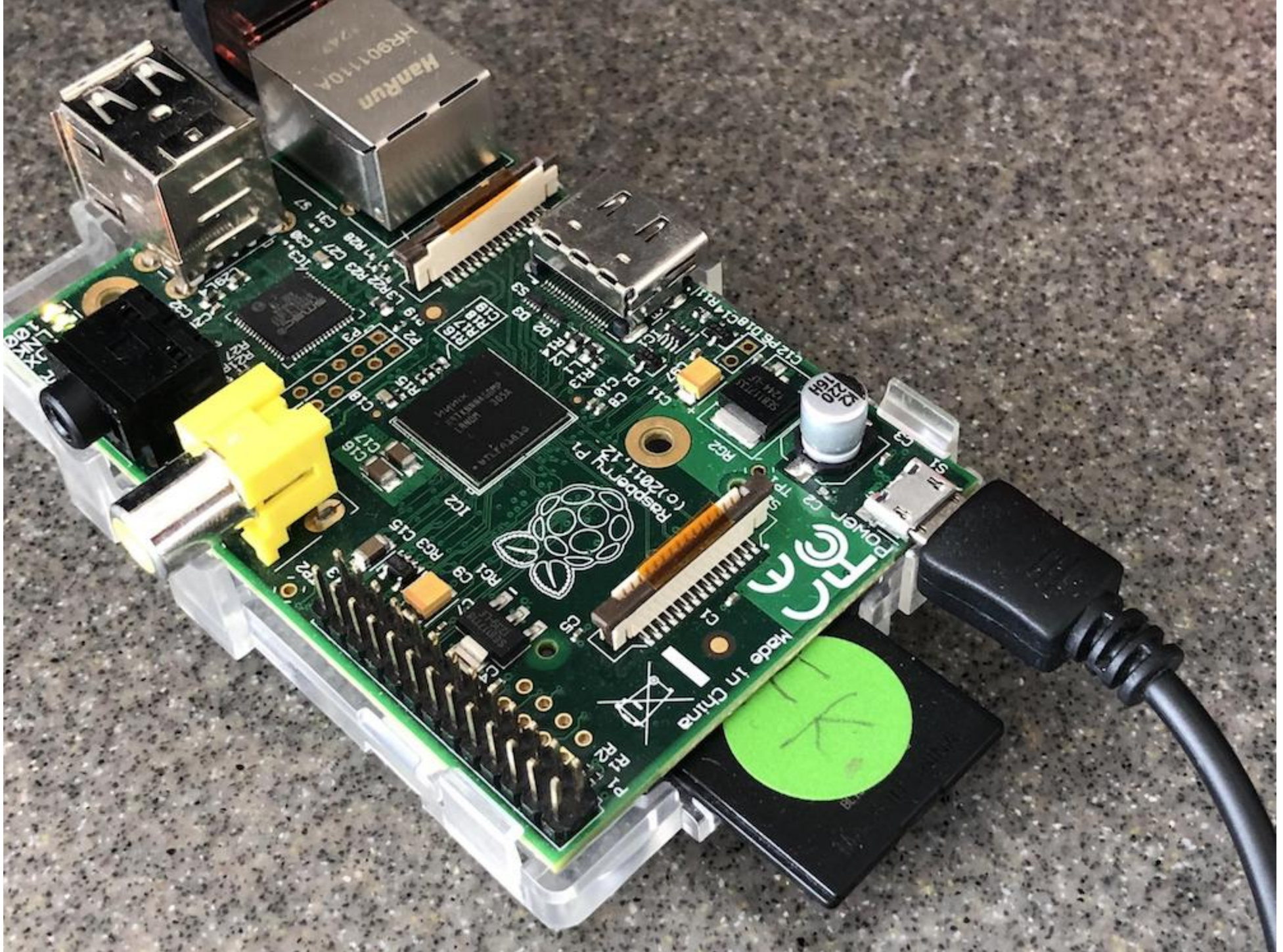

```
<?xml Version="1.0" Encoding="UTF-8"?>
<!doctype plist PUBLIC "-//Apple//DTD PLIST 1.
<plist Version="1.0">
<dict>
    <key>BuildMachineOSBuild</key>
    <string>16F73</string>
    <key>CFBundleDevelopmentRegion</key>
    <string>en</string>
    <key>CFBundleExecutable</key>
    <string>Localytics</string>
    <key>CFBundleIdentifier</key>
    <string>com.localytics.localytics</string>
    <key>CFBundleInfoDictionaryVersion</key>
    <string>6.0</string>
    <key>CFBundleName</key>
    <string>Modified by KrauseFx</string>
    <key>CFBundlePackageType</key>
    <string>FMWK</string>
    <key>CFBundleShortVersionString</key>
    <string>4.0.0</string>
```


Coffee, conference or hotel network
You
Attacker
Router
Internet


AWS | Mobile SDK – Mobile Ap
Secure https://aws.amazon.com/mobile/sdk/
Menu
aws
Contact Sales
Products
Solutions
Pricing
More
English
My Account
and easily. It provides easy access to a range of AWS services, including AWS Lambda, Amazon S3, Amazon DynamoDB, Amazon Mobile Analytics, Amazon Machine Learning, Elastic Load balancing, Auto Scaling and more.
The AWS Mobile SDK includes libraries, code samples, and documentation for iOS, Android, Fire OS, and Unity so you can build apps that deliver great experiences across devices and platforms.
PRODUCTS & SERVICES
AWS Mobile Hub
Mobile Partner Solutions
RELATED LINKS
AWS Mobile Hub
Amazon Cognito
Amazon Pinpoint
Amazon SNS Mobile Push
AWS Lambda
Get Started for Free
Create Free Account
AWS Mobile SDK: iOS 8 & above
iOS SDK
Get the source on GitHub
Developer Guide
AWS Mobile SDK: Android/Fire OS
Android SDK
Get the source on GitHub
Developer Guide

Official popup	Phishing popup
	


mim-demo
iPhone 6s
Running mim-demo on iPhone 6s
mim-demo
General
Capabilities
Resource Tags
Info
Build Settings
Build Phases
Build Rules
PROJECT
mim-demo
TARGETS
mim-demo
Bundle Identifier
com.krausefx.mim-demo
Version
1.0
Build
1
Signing
Automatically manage signing
Xcode will create and update profiles, app IDs, and certificates.
Team
Felix Krause (Individual - apple@krausefx.com)
Provisioning Profile
Xcode Managed Profile
Signing Certificate
iPhone Developer: Felix Krause (257GJD984M)
Deployment Info
Deployment Target
11.1
Devices
Universal
Main Interface
Main
Device Orientation
Portrait
Upside Down
Landscape Left
Landscape Right
Status Bar Style
Default
Hide status bar
Requires full screen
App Icons and Launch Images
App Icons Source
AppIcon
Launch Images Source
Use Asset Catalog...
AppDelegate.h
AppDelegate.m
ViewController.h
ViewController.m
Main.storyboard
Assets.xcassets
LaunchScreen.storyboard
Info.plist
main.m
Products
Carrier
4:38 PM
Thursday
23
Calendar
Photos
Maps
News
Reminders
Health
Wallet
Settings


HanRun
Raspberry Pi
(c)2011.12
Made in China
POWER

How to integrate buddybuild's

Felix

https://docs.buddybuild.com/quickstart/integrate_sdk.html

Update the SDK

1. Open the Terminal and `cd` to your root directory of your repo.
2. Run the following command:

```
curl -Ls http://tools.buddybuild.com/UpdateSDK | sh
```

3. Commit and push the changes.

Prefer to manually integrate the SDK?

Follow the Manual SDK Integration Guide.

Update the SDK

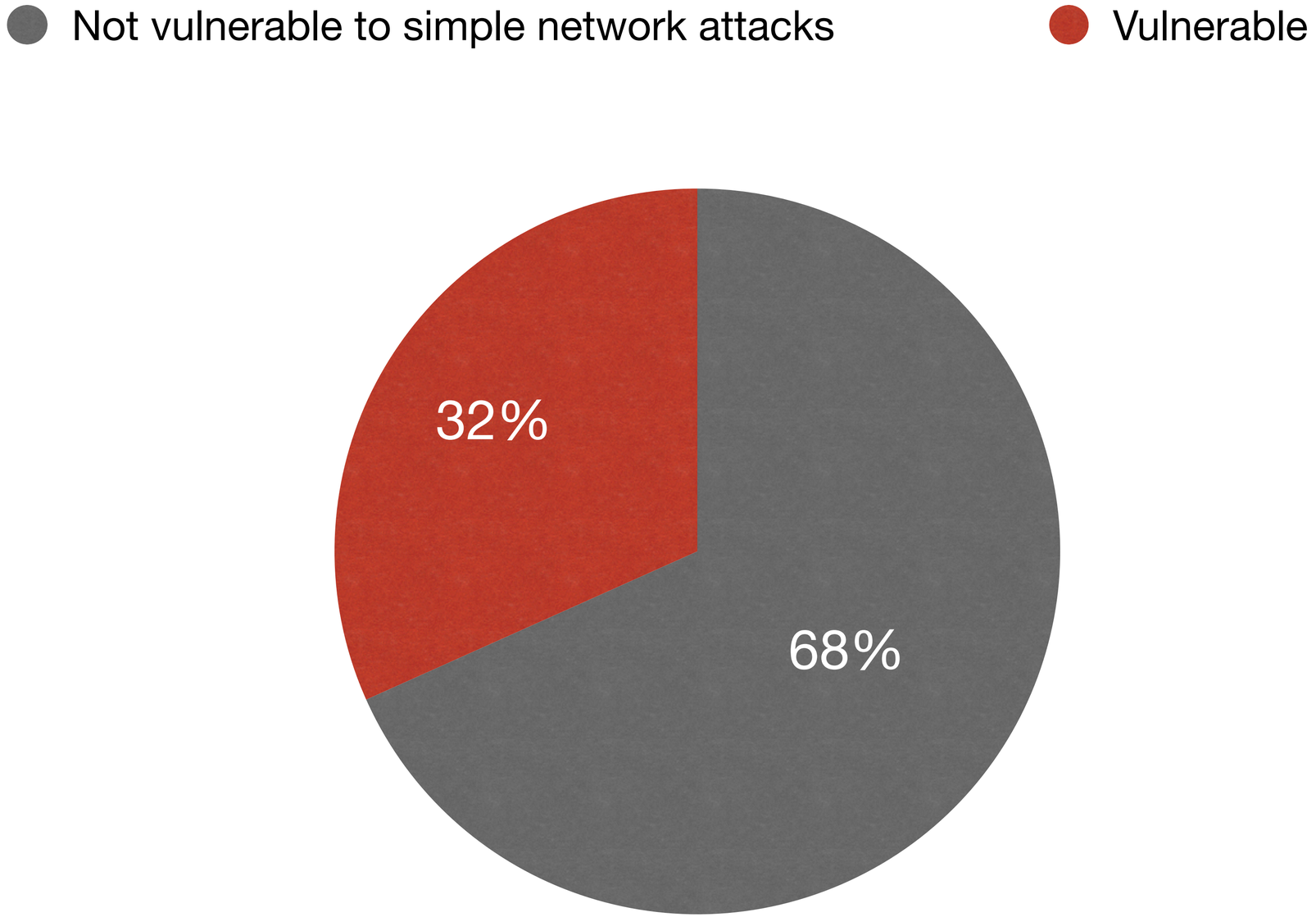
1. Open the Terminal and `cd` to your root directory of your repo.
2. Run the following command:

```
curl -Ls tools.buddybuild.com.s3-website-us-west-2.amazonaws.com/UpdateSDK |
 sh
```

3. Commit and push the changes.

Uninstall the SDK

If for some reason, you wish to uninstall the SDK, you simply need to revert the commit which installed it in the first place.


Not vulnerable to simple network attacks
Vulnerable
32%
68%

SDK providers’ reaction time

1 resolved within 3 days

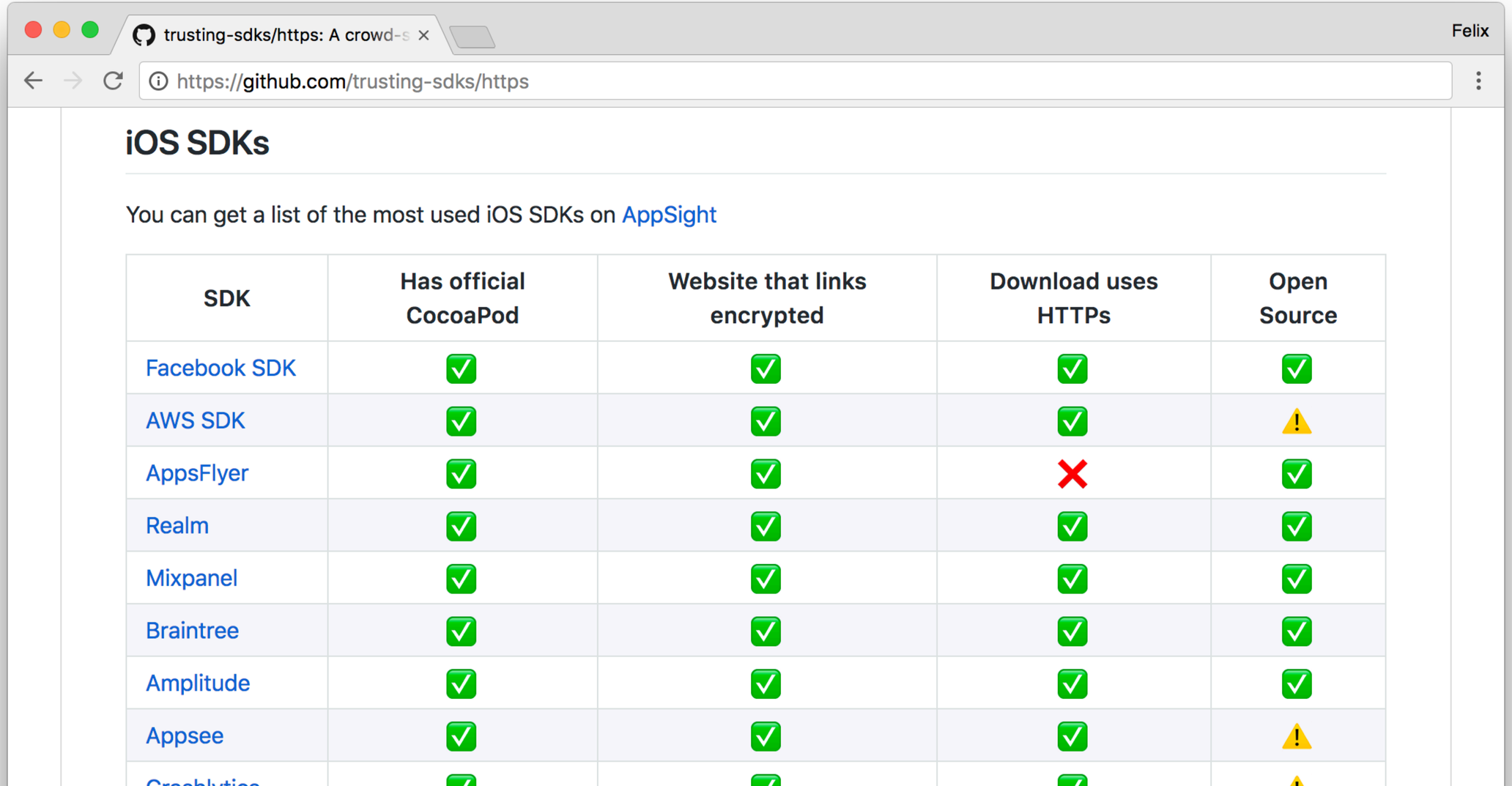
5 resolved within 1 month

2 resolved within 6 months

5 unresolved to this day

Open Source vs Closed Source

github.com/trusting-sdks/https



iOS SDKs

You can get a list of the most used iOS SDKs on AppSight

SDK	Has official CocoaPod	Website that links encrypted	Download uses HTTPs	Open Source
Facebook SDK	✅	✅	✅	✅
AWS SDK	✅	✅	✅	⚠️
AppsFlyer	✅	✅	❌	✅
Realm	✅	✅	✅	✅
Mixpanel	✅	✅	✅	✅
Braintree	✅	✅	✅	✅
Amplitude	✅	✅	✅	✅
Appsee	✅	✅	✅	⚠️

@KrauseFx