



# **How to Frida Good**

**Kevin Cody**  
**March 14, 2019**



# Goals

- Intro
- Mobile Testing Overview
- Tools of Yesteryear
- What is Frida
- Getting Started with Frida
- Tooling Based on Frida
- Demos
- Q&A



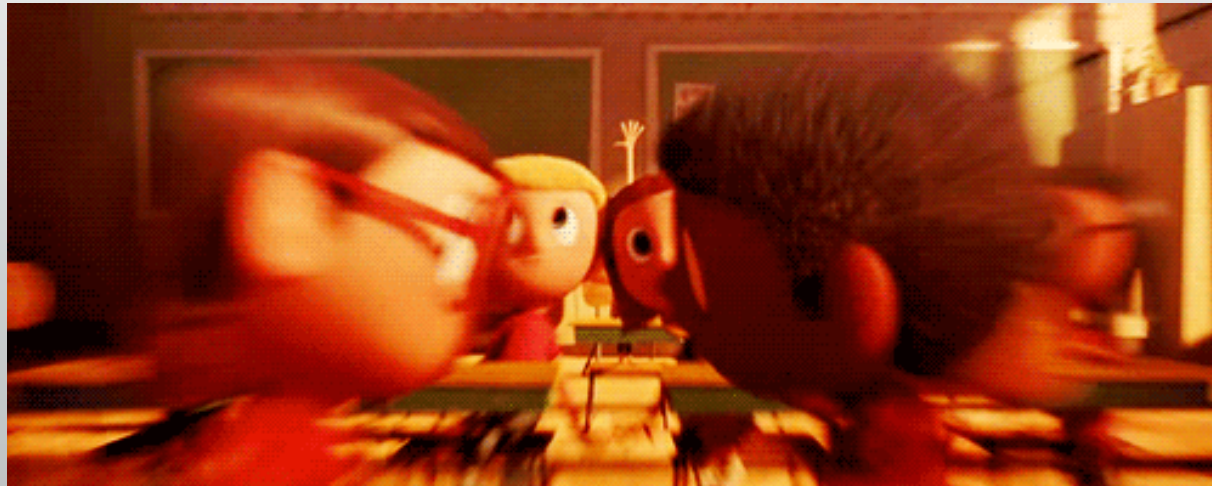
# Bio

- Kevin Cody
- @kevcody
- Principal Application Security Consultant at nVisium
- Mobile, IOT, Web, Mainframe
- Chapter Leader of OWASP Pittsburgh
- Speaking at OWASP Global AppSec Tel Aviv!



# Obligatory Polling Question

- Pentesters, Vulnerability Analysts, Security Folk? Bug Hunters?
- Developers?
- Auditors/Compliance?
- App Security is cool, yea?





# Mobile Testing

- Local Storage
- Client-Side Security
- Intellectual Property
- Memory
- Inter-Process Communication
- Transit Layer Protocol



# Tools of Yesteryear





# cycrypt

Cycrypt allows developers to explore and modify running applications on either iOS or Mac OS X using a hybrid of Objective-C++ and JavaScript syntax through an interactive console that features syntax highlighting and tab completion. (It also runs standalone on Android and Linux and provides access to Java, but without injection.)

current version: 0.9.594

[Download SDK](#)

[Read Manual](#)

Inject Into Processes

```
bash# cycrypt -p SpringBoard
```

Objective-C Messages

```
cy# [UIApplication]
```

JavaScript Extensions

```
cy# [for (x of [1,2,3]) x+1]
```



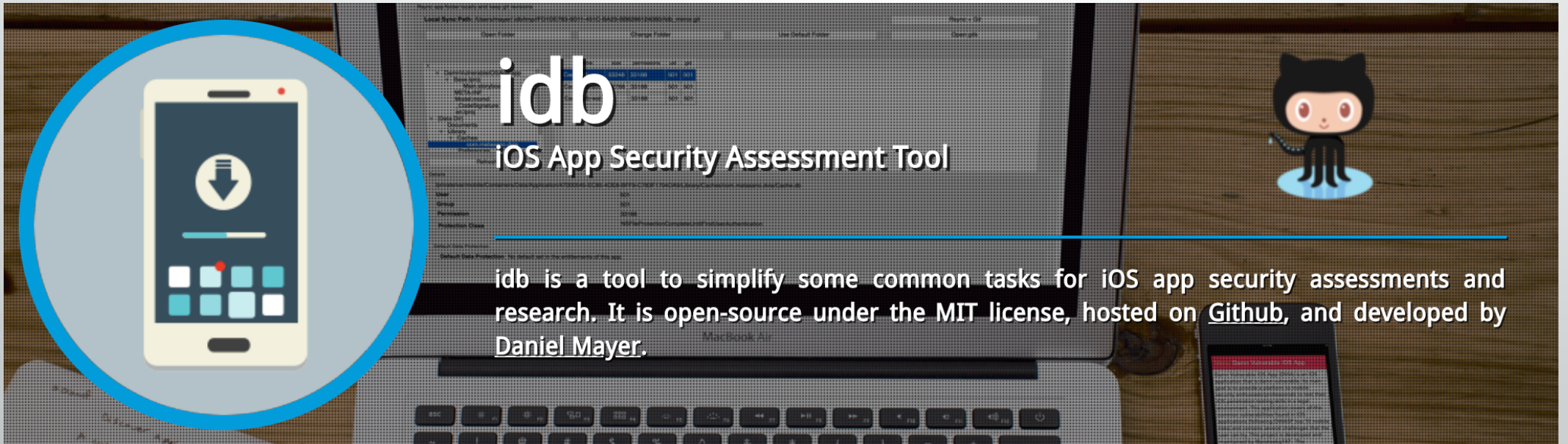
needle





drozer





A graphic for the 'idb' tool. It features a central laptop with a terminal window showing code. To the left is a circular icon of a smartphone with a download arrow. To the right is a GitHub Octocat mascot. The text 'idb' is prominently displayed in the center, with 'iOS App Security Assessment Tool' below it. A paragraph of text describes the tool's purpose and licensing.

**idb**  
iOS App Security Assessment Tool


idb is a tool to simplify some common tasks for iOS app security assessments and research. It is open-source under the MIT license, hosted on [Github](#), and developed by Daniel Mayer.



●●●●● TATA DOCOMO  12:04 am 



[< Settings](#) **SSL Kill Switch**

---

**Disable Certificate Validation** 


SSL Kill Switch v0.5 - iSEC Partners




Snoop-it MethodSwizzlingDemo  Connection Status: 

- Monitoring
  - Filesystem
  - Keychain
  - Network
  - Sensitive API
- Analysis
  - Objective-C Classes
  - View Controller
  - URL Schemes
- Runtime Manipulation
  - Hardware Identifier
  - Fake Location
  - Method Tracing

Home



Bundle Identifier:	Prateek.MethodSwizzlingDemo
Display Name:	MethodSwizzlingDemo
Version:	1.0
Build Version:	1.0
Has PIE:	true



Debug Report Search:

The screenshot shows the Snoop-it application interface. On the left is a sidebar with a tree view of monitoring and analysis categories. The main area is titled 'Home' and contains a table of metadata for the selected application. To the right of the table is a cartoon illustration of a white dog wearing a brown hat and a yellow scarf, holding a magnifying glass. At the bottom, there is a 'Debug Report' button and a search bar.



So.... now what?



**FRIIDA**



# Frida Author

- Ole André V. Ravnås
- [@oleavr](https://twitter.com/oleavr)
- Telegram channel: <https://t.me/fridadotre>  
Bridged to IRC: [#frida](https://irc.freenode.net) at irc.freenode.net
- Twitter: [@fridadotre](https://twitter.com/fridadotre)



# What *IS* Frida?

- Dynamic instrumentation toolkit for developers, reverse-engineers, and security researchers.
  - Scriptable
  - Portable
  - Free
  - Battle-tested





# Frida: Under the Covers

- Frida's core is written in C and injects Google's V8 engine into the target processes, where your JS gets executed with full access to memory, hooking functions and even calling native functions inside the process. There's a bi-directional communication channel that is used to talk between your app and the JS running inside the target process.

*(<https://www.frida.re/docs/home/>)*



# Basic Frida skills

- Attaching to Processes
- Function Hooking
- Modifying Function Arguments
- Calling Functions
- Inspecting memory
- Modifying memory

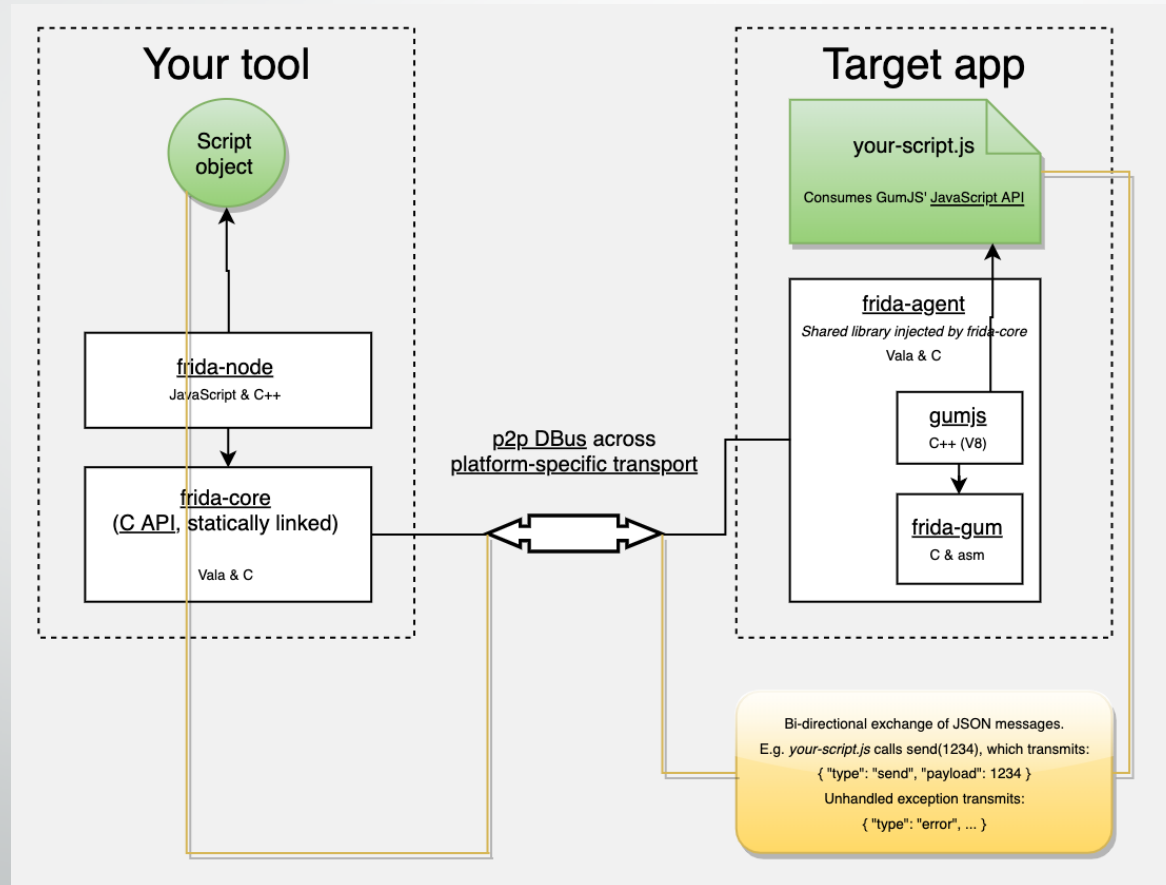


# Basic Components

- Frida Server
- Frida Client
  - Daemon
  - Gadget
- Native OS Tooling



# Basic Frida Architecture



(<https://www.frida.re/docs/hacking/>)



# Root/Jailbreak Required?



# GOTO Devices

- Android
  - Google Pixel (Nexus)
  - Motorola
  - OnePlus\*
- iOS
  - Whatever the tooling supports
  - Insider Tip





# Supported Operating Systems

- Windows
- macOS
- QNX
- iOS
- Android





# Installation

- PyPi (pip3)
- Releases via GitHub
- Cydia
- adb/scp push





# Smoke Test

- Use frida-ps and frida-ps -u
- Make sure:
  - Devices are connected
  - adb is running
  - Frida daemon is running
  - USB-C connection is the correct orientation :)



# Useful Scripts and Tooling

- FriDump – Python Script that dumps device memory
- Objection - Runtime mobile exploration
- Passionfruit - Simple iOS app blackbox assessment tool. Powered by Frida and vue.js



# Frida CodeShare

Frida CodeShare [Twitter](#) [GitHub](#) Log In

---

## Projects by popularity

### Universal Android SSL Pinning Bypass with Frida

👍 13 | 👁 23K

Uploaded by: [@pcipolloni](#)

Android SSL Re-Pinning, more information can be found here <https://techblog.mediaservice.net/2017/07/universal-android-ssl-pinning-bypass-with-frida/>

[PROJECT PAGE](#)

### iOS DataProtection

👍 7 | 👁 2K

Uploaded by: [@ay-kay](#)

List iOS file data protection classes (NSFileProtectionKey) of an app

[PROJECT PAGE](#)

### ObjC method observer

👍 4 | 👁 2K

Uploaded by: [@mrmacete](#)

Observe all method calls to a specific class (e.g. observeClass('LicenseManager')), or dynamically resolve methods to observe using ApiResolver (e.g. observeSomething("[\* \*Password:\*]")). The script tries to do its best to resolve and display input parameters and return value. Each call log comes with its stacktrace.

[PROJECT PAGE](#)

### ios-app-info

👍 3 | 👁 1K

Uploaded by: [@dki](#)

Dump useful information for an iOS app

[PROJECT PAGE](#)

### aesinfo

👍 3 | 👁 1K

Uploaded by: [@dzonerzy](#)

Show useful info about AES encryption/decryption at application runtime

[PROJECT PAGE](#)

### fridantiroot

👍 3 | 👁 9K

Uploaded by: [@dzonerzy](#)

Android antiroot checks bypass

[PROJECT PAGE](#)



DEMO TIME



# Summary

- Frida is awesome!
- The very nature and power of the tool has created frameworks that have replaced and surpassed legacy tooling.
- Utilize CodeShare and/or Frida frameworks as a baseline.
- Don't be afraid to crash and burn.
- When in doubt, purge and reinstall the app.



Questions?

# References

- <https://www.frida.re/>
- <https://www.frida.re/docs/presentations/osdc-2015-putting-the-open-back-into-closed-software.pdf>