



**CISPA**  
HELMHOLTZ-ZENTRUM I. G.



Oliver Schranz

# ARTist - A Novel Instrumentation Framework for Reversing and Analyzing Android Apps and the Middleware

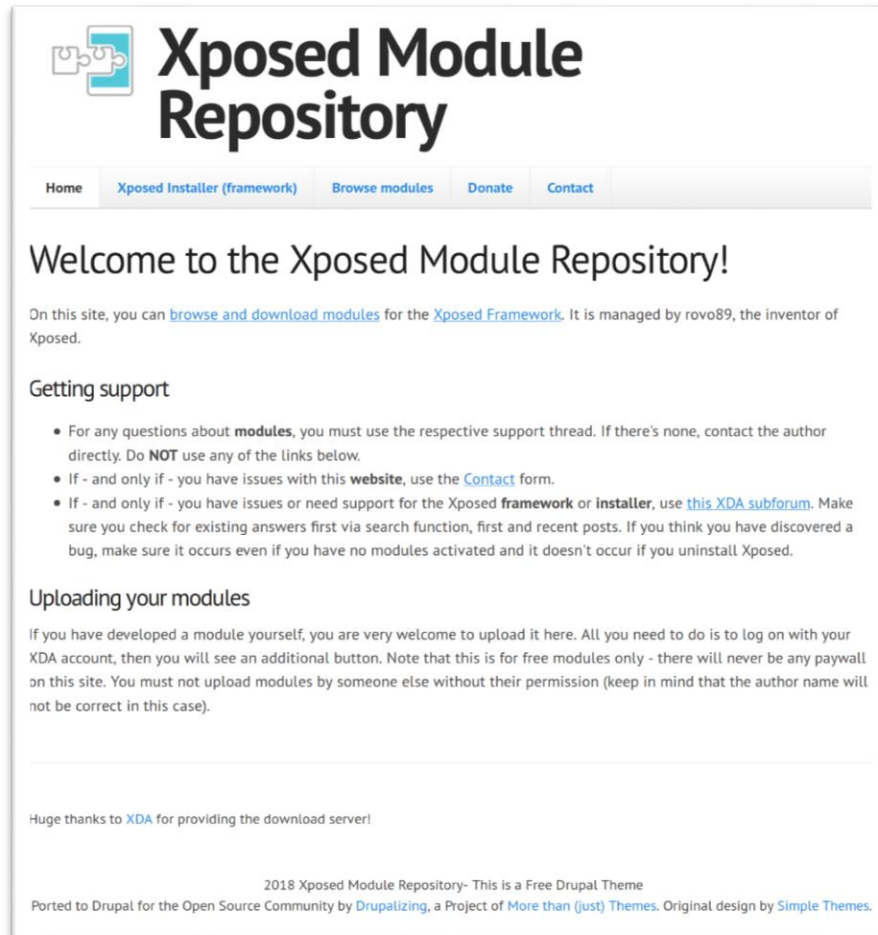
Joint work with Sebastian Weisgerber, Sven Bugiel, Jie Huang, Michael Backes, Alexander Fink, Parthipan Ramesch, Maximilian Jung

## \$ whoami

- Ph.D. student at CISP Helmholtz Center i.G.
- Research focus: Android security solutions
- Software Engineer and (occasionally) penetration tester at Backes SRT GmbH
- Founding member of saarsec CTF team (Saarland University)
- Conference attendee & speaker: CCS, USENIX Sec, EuroS&P, Droidcon, Black Hat
- Passionate about almost any security-related topic!

# App Instrumentation & Dynamic Analysis

There are already Xposed and Frida, so why bother?



The screenshot shows the Xposed Module Repository website. It features a logo with puzzle pieces and the title 'Xposed Module Repository'. A navigation bar includes links for Home, Xposed Installer (framework), Browse modules, Donate, and Contact. The main heading is 'Welcome to the Xposed Module Repository!'. Below it, a paragraph explains that users can browse and download modules for the Xposed Framework, managed by rovo89. A 'Getting support' section lists three bullet points: using support threads for modules, contacting the author directly for website issues, and using the XDA subforum for framework or installer issues. An 'Uploading your modules' section welcomes users to upload their own modules. At the bottom, there is a thank you message to XDA and footer text about the website being a free Drupal theme ported to Drupal.

**Xposed Module Repository**

Home Xposed Installer (framework) Browse modules Donate Contact

## Welcome to the Xposed Module Repository!

On this site, you can [browse and download modules](#) for the [Xposed Framework](#). It is managed by rovo89, the inventor of Xposed.

### Getting support

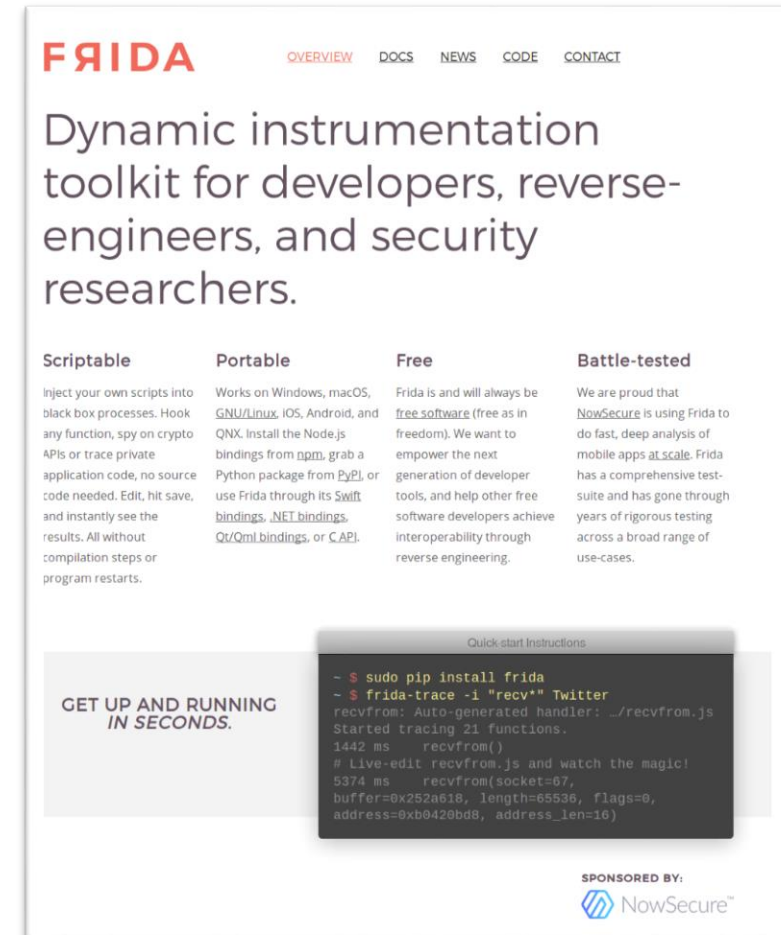
- For any questions about **modules**, you must use the respective support thread. If there's none, contact the author directly. Do **NOT** use any of the links below.
- If - and only if - you have issues with this **website**, use the [Contact](#) form.
- If - and only if - you have issues or need support for the Xposed **framework** or **installer**, use [this XDA subforum](#). Make sure you check for existing answers first via search function, first and recent posts. If you think you have discovered a bug, make sure it occurs even if you have no modules activated and it doesn't occur if you uninstall Xposed.

### Uploading your modules

If you have developed a module yourself, you are very welcome to upload it here. All you need to do is to log on with your XDA account, then you will see an additional button. Note that this is for free modules only - there will never be any payoff on this site. You must not upload modules by someone else without their permission (keep in mind that the author name will not be correct in this case).

Huge thanks to [XDA](#) for providing the download server!

2018 Xposed Module Repository- This is a Free Drupal Theme  
Ported to Drupal for the Open Source Community by [Drupalizing](#), a Project of [More than \(just\) Themes](#). Original design by [Simple Themes](#).



The screenshot shows the Frida website. It features the 'FRIDA' logo in red and a navigation bar with links for Overview, Docs, News, Code, and Contact. The main heading is 'Dynamic instrumentation toolkit for developers, reverse-engineers, and security researchers'. Below this, four columns describe the toolkit's features: Scriptable (injecting scripts into black box processes), Portable (works on Windows, macOS, GNU/Linux, iOS, Android, and QNX), Free (free software), and Battle-tested (used by NowSecure). A 'Quick start instructions' box shows terminal commands for installing Frida and tracing a function. At the bottom, it says 'SPONSORED BY: NowSecure'.

**FRIDA** Overview Docs News Code Contact


## Dynamic instrumentation toolkit for developers, reverse-engineers, and security researchers.

<b>Scriptable</b> Inject your own scripts into black box processes. Hook any function, spy on crypto APIs or trace private application code, no source code needed. Edit, hit save, and instantly see the results. All without compilation steps or program restarts.	<b>Portable</b> Works on Windows, macOS, GNU/Linux, iOS, Android, and QNX. Install the Node.js bindings from npm, grab a Python package from PyPI, or use Frida through its Swift bindings, .NET bindings, Qt/Qtml bindings, or C API.	<b>Free</b> Frida is and will always be <a href="#">free software</a> (free as in freedom). We want to empower the next generation of developer tools, and help other free software developers achieve interoperability through reverse engineering.	<b>Battle-tested</b> We are proud that <a href="#">NowSecure</a> is using Frida to do fast, deep analysis of mobile apps at <a href="#">scale</a> . Frida has a comprehensive test-suite and has gone through years of rigorous testing across a broad range of use-cases.
--	---	---	---

Quick start instructions

```
- $ sudo pip install frida
- $ frida-trace -i "recv*" Twitter
recvfrom: Auto-generated handler: ../recvfrom.js
Started tracing 21 functions.
1442 ms   recvfrom()
# Live-edit recvfrom.js and watch the magic!
5374 ms   recvfrom(socket=67,
buffer=0x252a618, length=65536, flags=0,
address=0xb0420bd8, address_len=16)
```

GET UP AND RUNNING IN SECONDS.

SPONSORED BY:  NowSecure™

# Xposed & Frida: Disadvantages

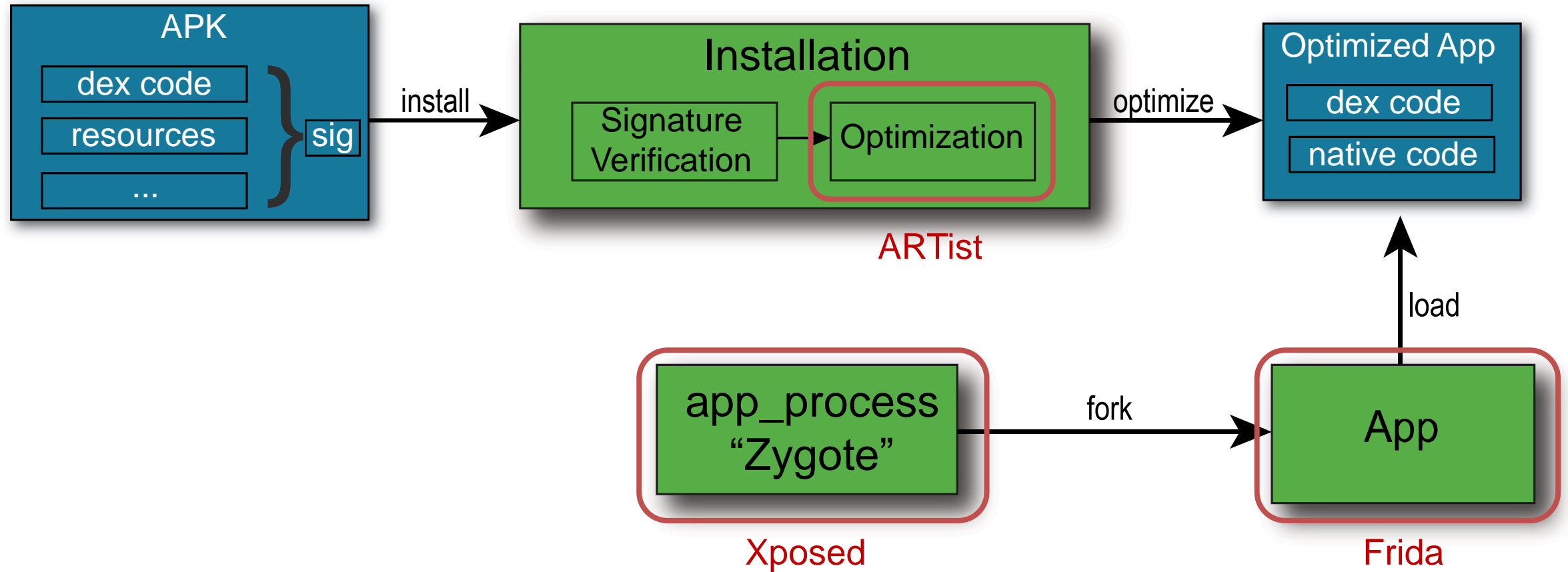
## ***Xposed***

- Replaces *app\_process (Zygote)*
    - + **Hooks**: Apps *and* systemserver
    - **Performance**: Intercept *all* methods
    - **Granularity**: Method hooks
    - **Security**: All modules in all targets
  - Flashed via custom recovery
    - **Unlocked bootloader**
    - **Deep OS modification**
- *Persistent modifications for power users*

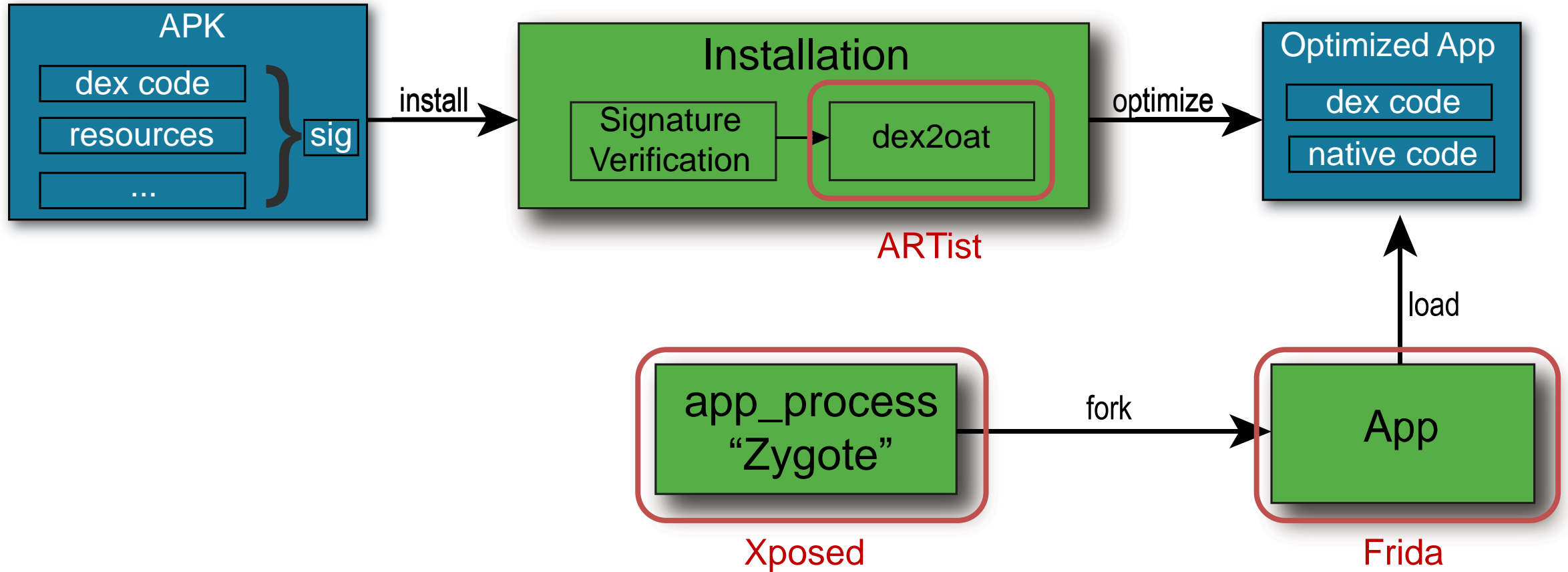
## ***Frida***

- Injects JS VM into process memory
    - + **Hooks**: *Any* process
    - **Performance**: V8 overhead
    - **Granularity**: Method hooks
  - Deployed via Frida-server or Gadget
    - **SELinux patches or shutdown**
- *Temporary modifications for experts*

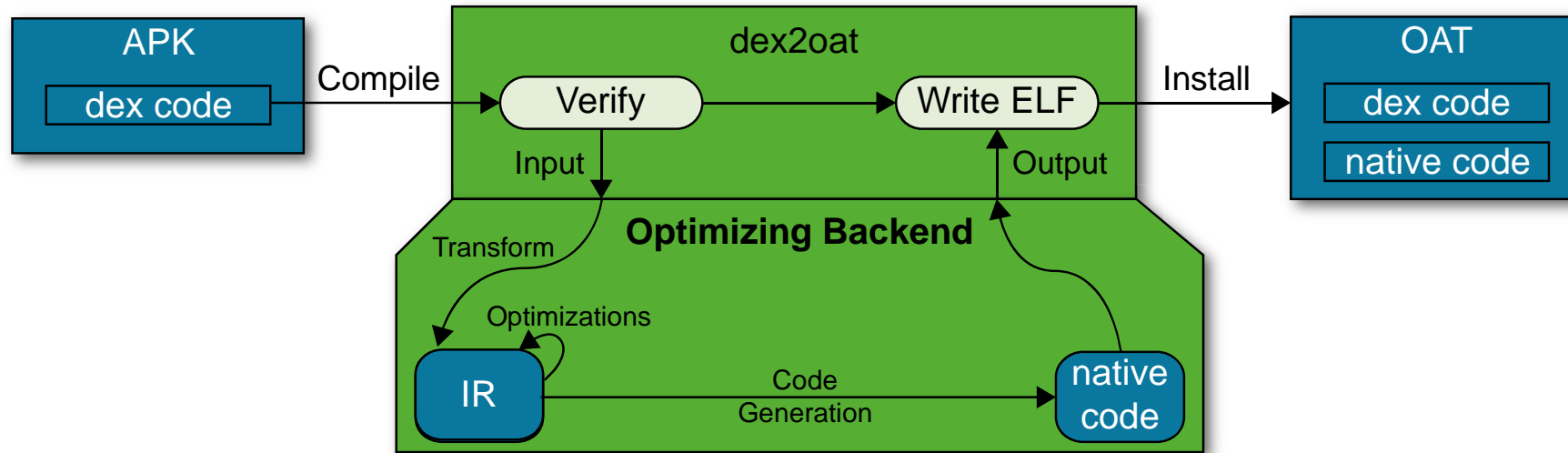
# Installation Process



# Installation Process

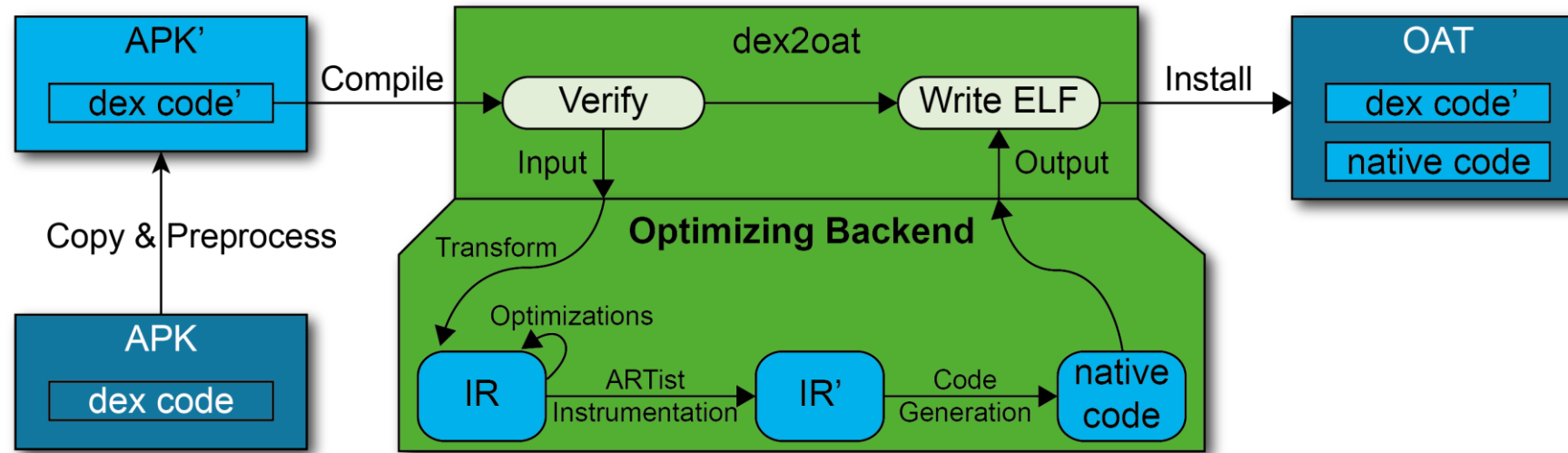


## ART & dex2oat



- State-of-the-art optimization framework
- Support for x86(64), arm(64) and mips(64)
- Output .oat file is a specialized ELF shared object

# ARTist – The Android Runtime instrumentation and security toolkit



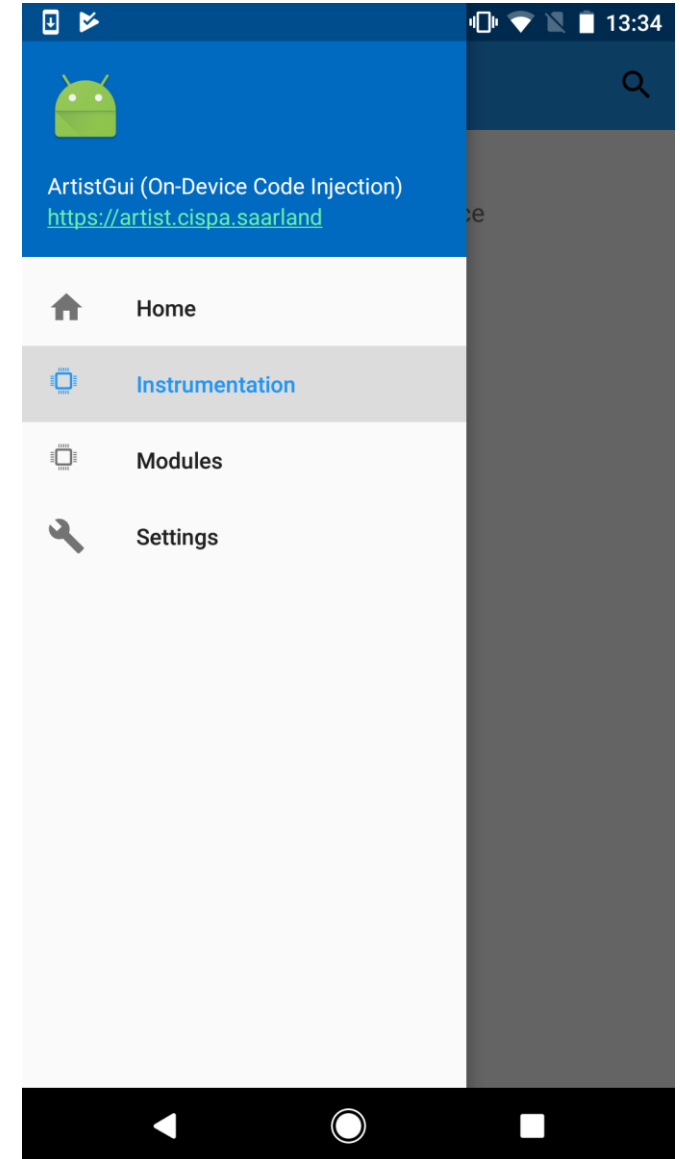
- App signature preservation (no repackaging)
- Close to no runtime overhead for instrumentation
- Non-intrusive/easily revertible
- Runs on rooted stock devices



# Deployment: App

## *ArtistGui*

- Regular Android app
- Run ARTist as a binary
- On-demand instrumentation of installed apps
- Keep apps instrumented upon updates
- Choose modules for each app
- Later: Automatic updates of ARTist and modules



## Framework Comparison

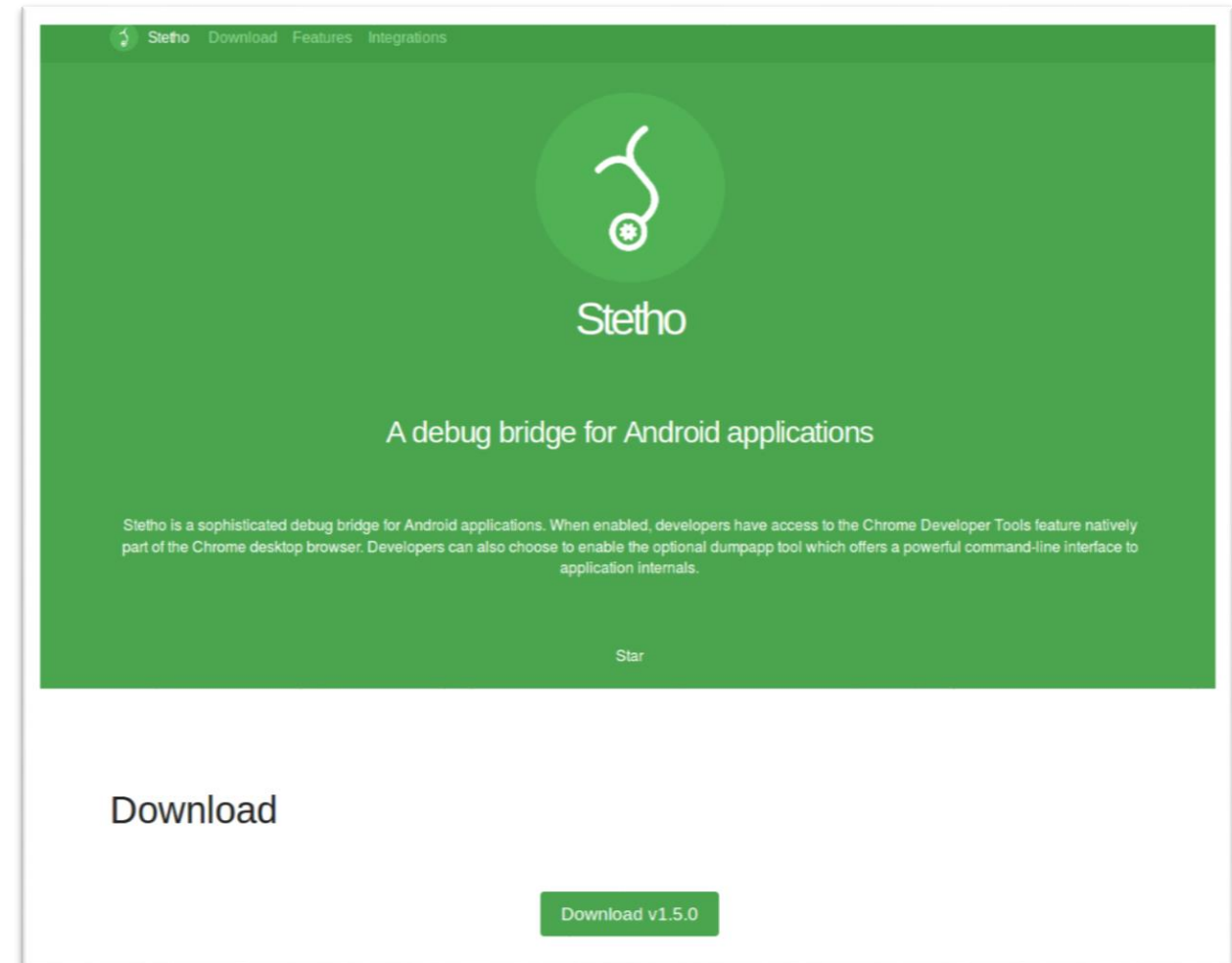
	Xposed	Frida	ARTist
Deployment	Custom recovery	adb + connected PC	App
Invasiveness	Modify OS	Modify Target Process	Change Compiled App
Granularity	Method	Method	Instruction
Module updates	Reboot	Instantaneous	Recompilation
Android Versions	4.1 - 8	4.2 - 8	6 - 8

ARTist aims for a sweet spot that combines ease of deployment and non-invasiveness with fine-grained instrumentation and a focus on experts *and* users

## Module: Stetho

- Stetho Debug Bridge
  - Intercept network traffic
  - Read and modify files
  - Access databases
  - Inspect and change layout
  - JS code exec in app context
- Meant to be included in debug build of own app

What if someone injects this into arbitrary third-party apps?



**DEMO**

# Advanced Usage

## *Other Modules*

- Intra-App Taint Tracking
- Ad Library Compartmentalization
- IRM-based Permission Refinement
- Method Tracing
- Test coverage for arbitrary apps
- ...

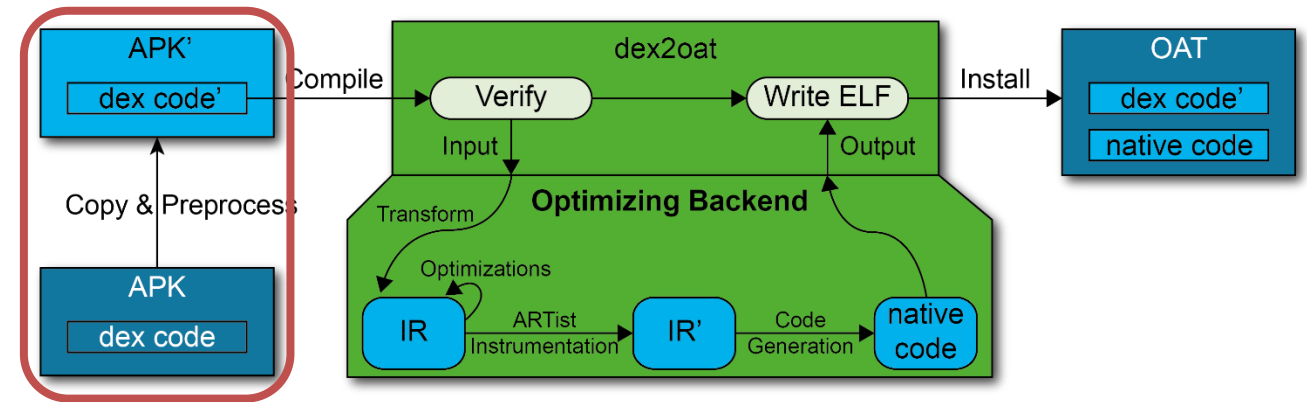
## *Replace system compiler*

- Custom ROM: ARTist as system compiler
- instrument apps, middleware & framework
- WIP: Recompile from ArtistGui

```
/system/bin/dex2oat
--zip-fd=6 --oat-fd=7
--zip-location=services.jar
--oat-location=/data/dalvik-cache/x86_64/
               system@framework@services.jar@classes.dex
--instruction-set=x86_64
--compiler-filter=everything
--instruction-set-features=default
...
```

# Modules

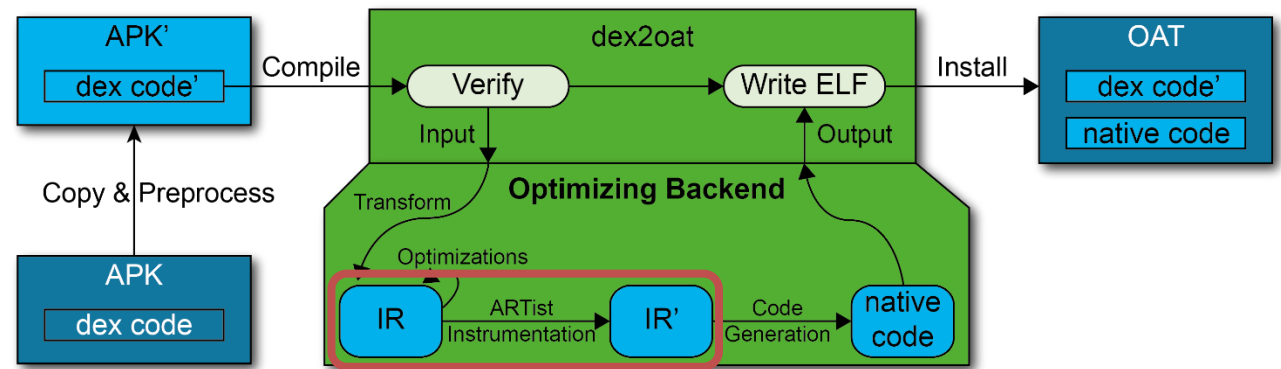
- What is an ARTist module?
  - CodeLib (.apk)
  - ARTist “optimization” passes (.so)
  - Manifest (.json)
    - Version
    - Maintainer
    - ...



- Self-contained package that represents an abstract functionality
- Contains everything needed by ArtistGui & ARTist to manage and execute your module
- Created using our Module SDK

# Modules

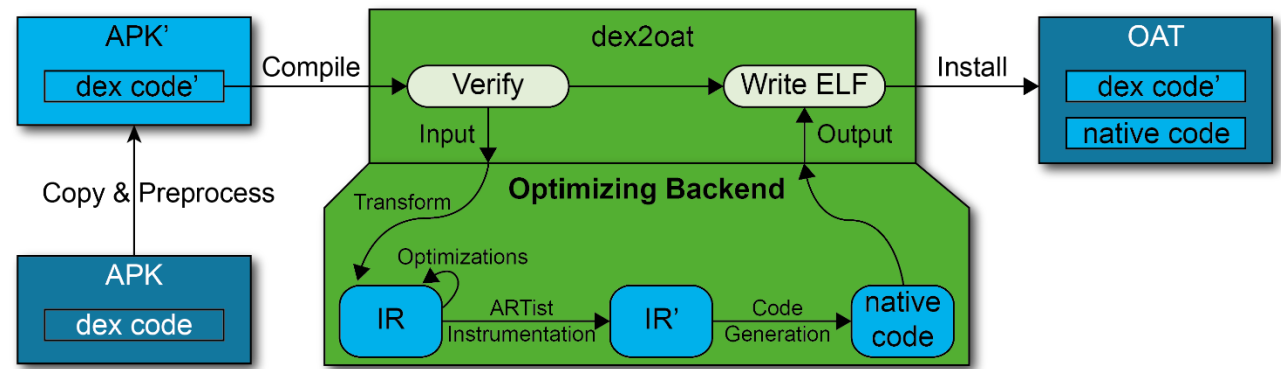
- What is an ARTist module?
  - CodeLib (.apk)
  - ARTist “optimization” passes (.so)
  - Manifest (.json)
    - Version
    - Maintainer
    - ...



- Self-contained package that represents an abstract functionality
- Contains everything needed by ArtistGui & ARTist to manage and execute your module
- Created using our Module SDK

# Modules

- What is an ARTist module?
  - CodeLib (.apk)
  - ARTist “optimization” passes (.so)
  - **Manifest (.json)**
    - Version
    - Maintainer
    - ...



- Self-contained package that represents an abstract functionality
- Contains everything needed by ArtistGui & ARTist to manage and execute your module
- Created using our Module SDK

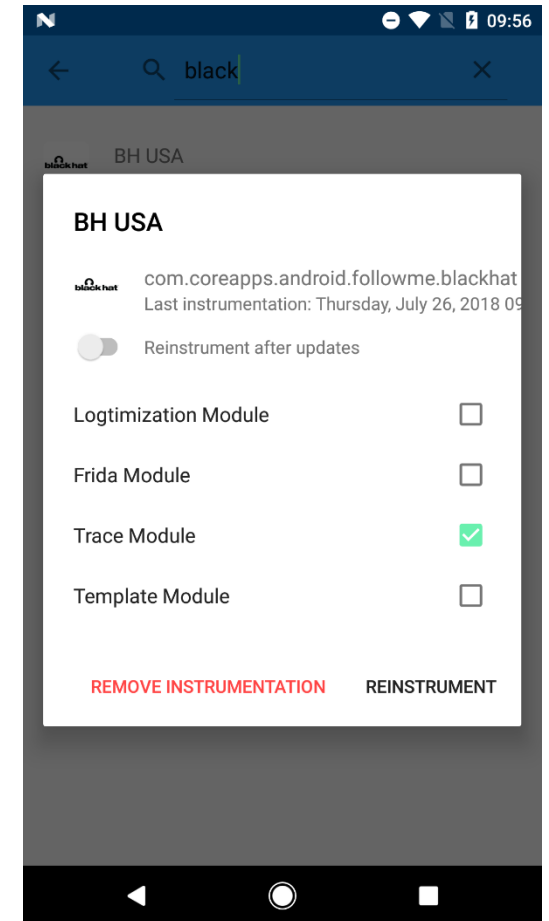


# Creating own modules

Basic workflow for the app deployment (system deployment differs)

1. Install SDK
2. Fork template-module & codelib
3. Implement your module
4. Build & deploy
5. Import in ArtistGui
6. Profit

More information at <https://artist.cispa.saarland>



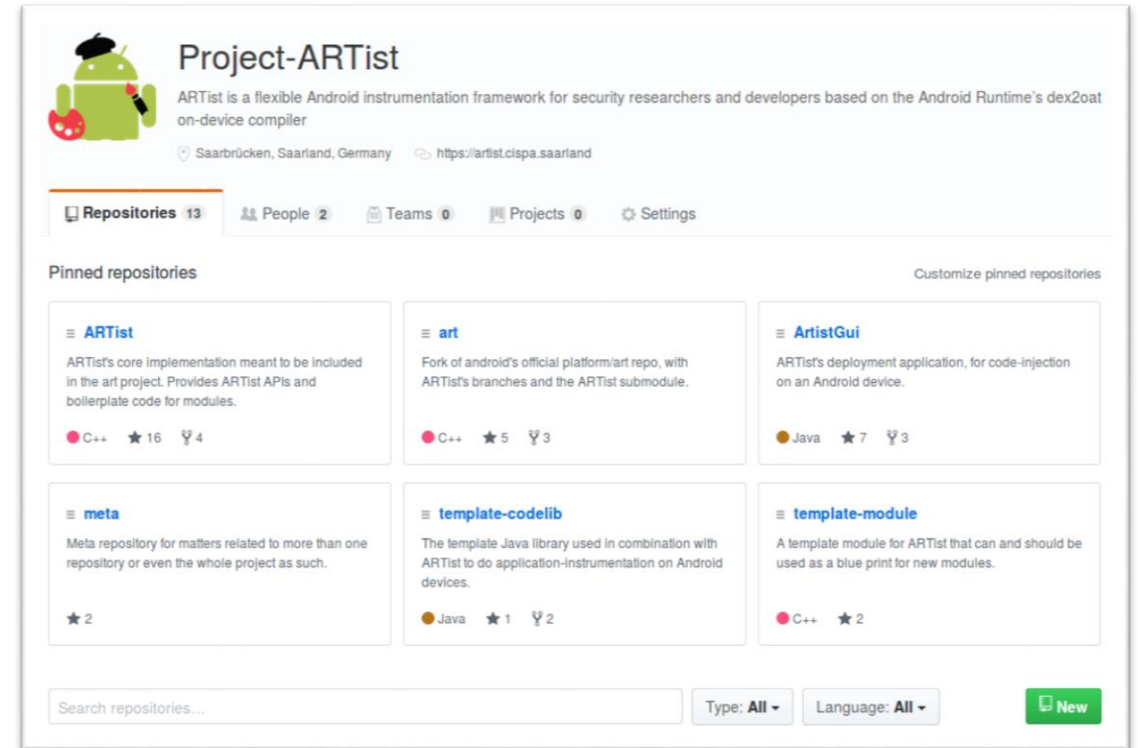
# Current State & Outlook

- We just entered the beta phase

- Artist Module SDK
- Module management in ArtistGui
- Semantic versioning
- Documentation v2

- Later™:

- Automated testing & release
- Public module marketplace
- Support for Xposed modules
- Systemserver and framework support for rooted stock devices?



1. Android instrumentation & analysis is fun
2. ARTist occupies a sweet spot among instrumentation frameworks
3. ARTist is open source & in beta, get involved!

If you are curious now, check out our Gitter & GitHub

 <https://gitter.im/project-artist/>  
 <https://github.com/Project-ARTist/>