目录

移动端调试利器：Objection

- 最新版本：`v1.0.0`
- 更新时间：`20230916`

简介

整理移动端调试利器，用Objection调试Android和iOS的程序。先是Objection的概览；然后是初始化开发环境；接着介绍通用逻辑，包括查看子命令的参数、hook函数的参数；然后是如何调试Android，主要包括android各种子命令，包括hooking、intent；而hooking下面有子命令list、watch、search；list下有子命令class_methods、class_method、services、activities、class_loaders；intent有子命令launch_activity；以及memory的各种子命令，包括search、dump；然后是调试iOS；以及常见问题，包括调试安卓的；最后给出附录，包括语法help、教程和资料。

源码+浏览+下载

本书的各种源码、在线浏览地址、多种格式文件下载如下：

HonKit源码

- crifan/mobile_reverse_debug_objection: 移动端调试利器：Objection

如何使用此HonKit源码去生成发布为电子书

详见：crifan/honkit_template: demo how to use crifan honkit template and demo

在线浏览

- 移动端调试利器：Objection book.crifan.org
- 移动端调试利器：Objection crifan.github.io

离线下载阅读

- 移动端调试利器：Objection PDF
- 移动端调试利器：Objection ePub
- 移动端调试利器：Objection Mobi

版权和用途说明

此电子书教程的全部内容，如无特别说明，均为本人原创。其中部分内容参考自网络，均已备注了出处。如发现有侵权，请通过邮箱联系我 `admin 艾特 crifan.com`，我会尽快删除。谢谢合作。

各种技术类教程，仅作为学习和研究使用。请勿用于任何非法用途。如有非法用途，均与本人无关。

鸣谢

感谢我的老婆**陈雪**的包容理解和悉心照料，才使得我 `crifan` 有更多精力去专注技术专研和整理归纳出这些电子书和技术教程，特此鸣谢。

其他

作者的其他电子书

本人 `crifan` 还写了其他 `150+` 本电子书教程，感兴趣可移步至：

crifan/crifan_ebook_readme: Crifan的电子书的使用说明

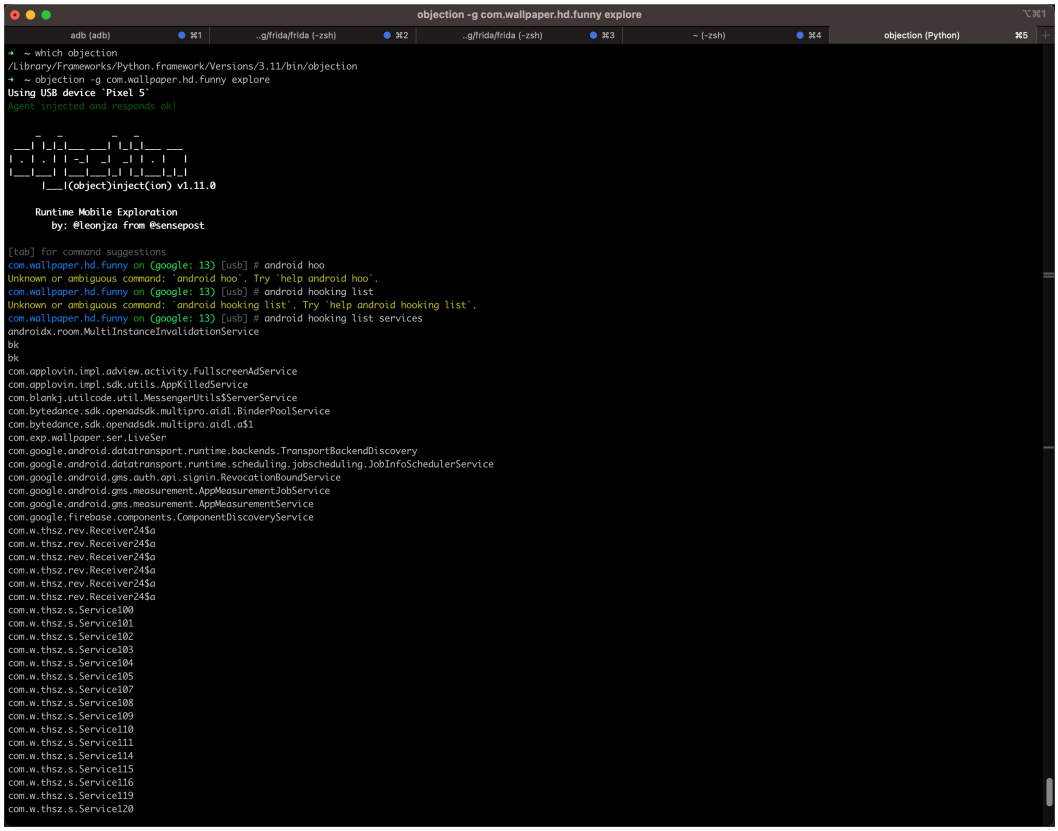
关于作者

关于作者更多介绍，详见：

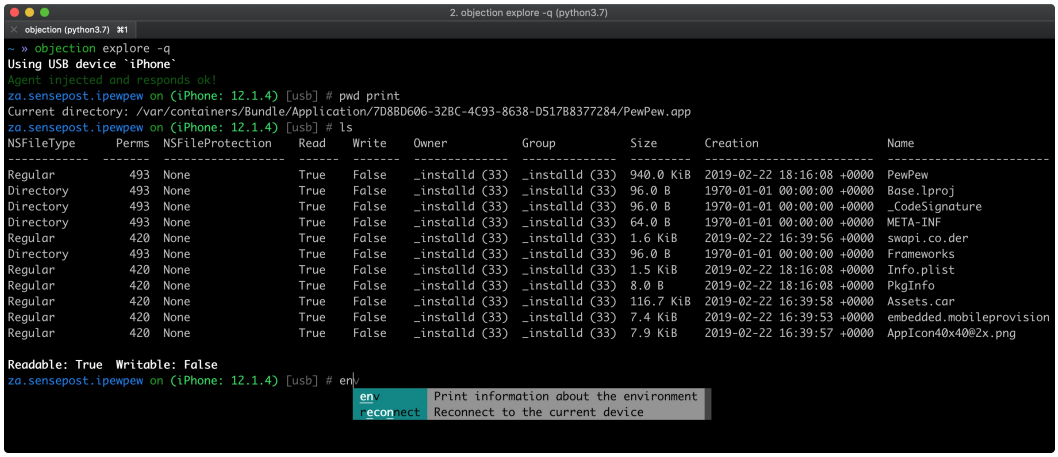
关于CrifanLi李茂 – 在路上

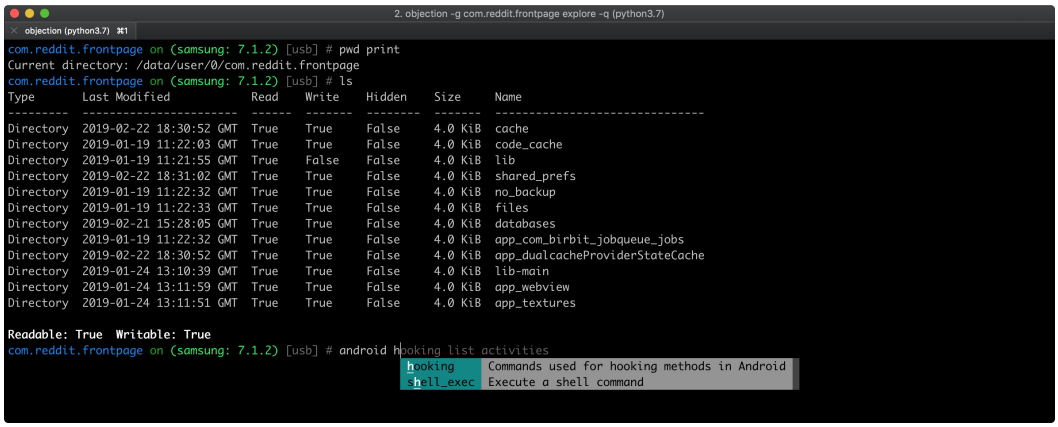
crifan.org，使用署名4.0国际(CC BY 4.0)协议发布 all right reserved，powered by Gitbook最后更新：2023-09-17 01:29:58

Objection概览

- `Objection`
  - 是什么：底层依赖于Frida的移动端（Android和iOS）的hook调试工具
  - 一句话概述：objection is a runtime mobile exploration toolkit, powered by Frida, built to help you assess the security posture of your mobile applications, without needing a jailbreak
  - 功能=特点
    - 支持iOS和Android
    - 支持查看和修改移动端的文件系统内容
    - 支持绕过SSL pinning=证书绑定（实现https抓包查看明文数据）
    - 支持导出keychains
    - 支持各种内存相关操作：dump导出、patching打补丁等
    - 支持操作Heap堆
    - 等等
  - Github
    - sensepost/objection:　　objection - runtime mobile exploration (github.com)
  - 截图
    - hook调试安卓
      - 

    - A file system listing of the iOS applications main bundle

- 

- A file system listing of the Android applications bundle
  - 

crifan.org，使用署名4.0国际(CC BY 4.0)协议发布 all right reserved，powered by Gitbook最后更新：2023-09-17 01:26:49

环境初始化

- Mac

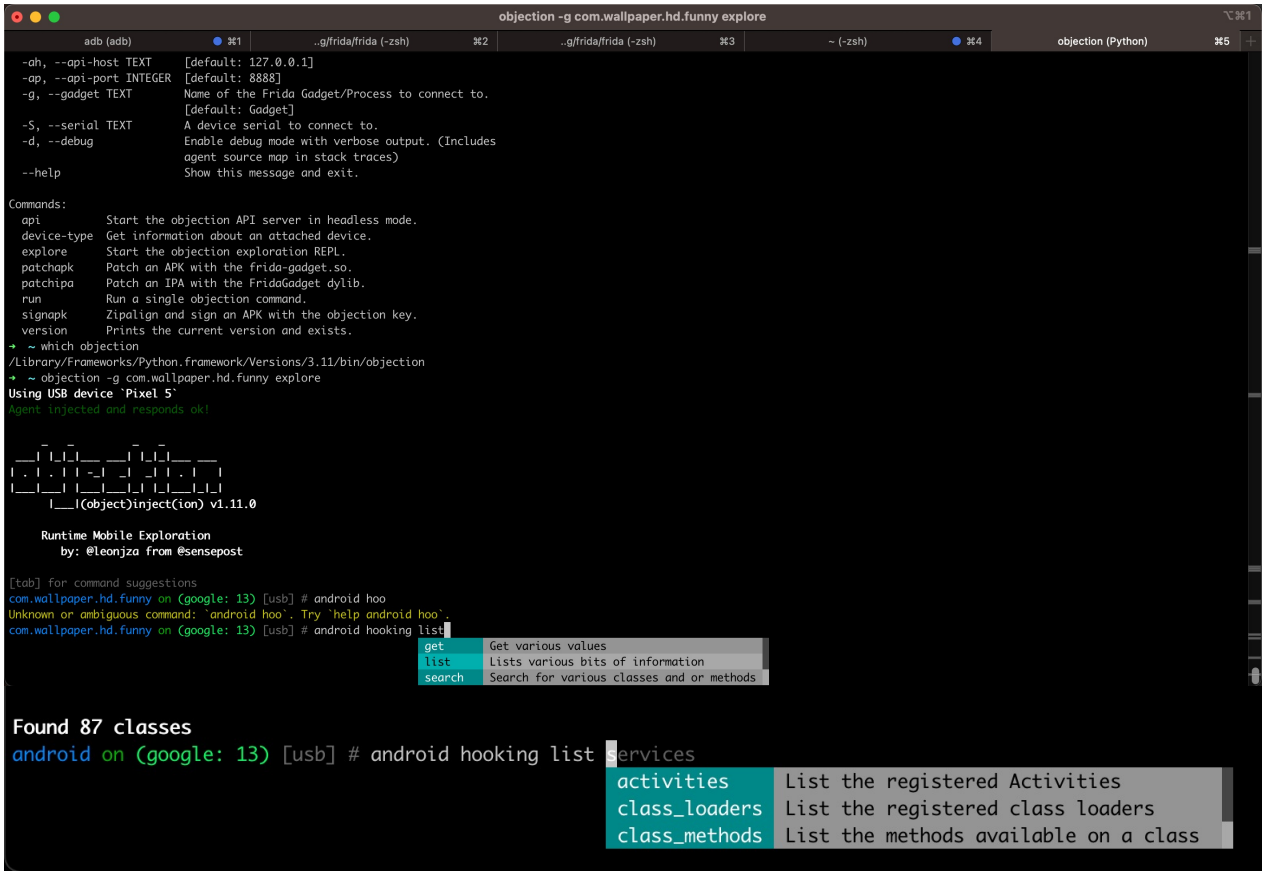
```
pip3 install objection
```

crifan.org，使用署名4.0国际(CC BY 4.0)协议发布 all right reserved，powered by Gitbook最后更新：2023-09-16 22:20:34

Objection基本用法

支持子命令的自动tab补全

当输入了对应命令后，后续会自动tab补全=显示有哪些子命令：



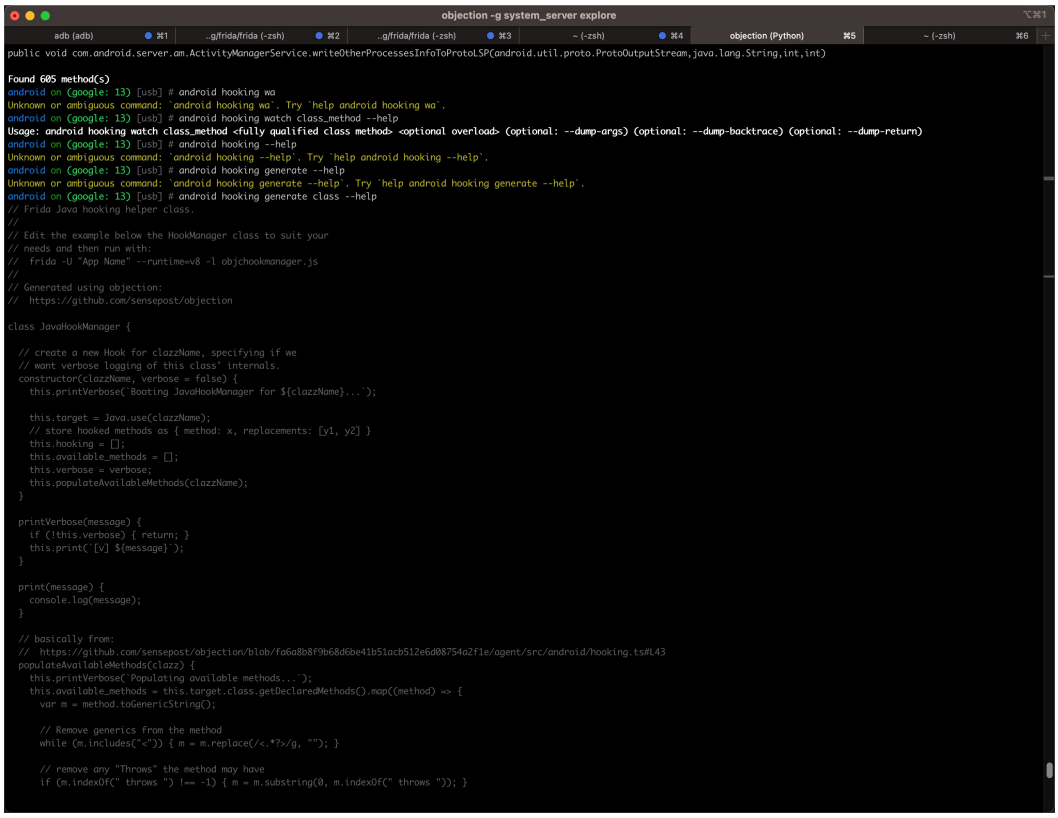
如此，即可靠自己，慢慢摸索出，常用的命令，以及后续的语法和子命令了。

crifan.org，使用署名4.0国际(CC BY 4.0)协议发布 all right reserved，powered by Gitbook最后更新：2023-09-17 01:10:23

Objection中查看子命令的参数

- 需求：Objection中，想要查看某个命令的子命令和参数
- 举例：子命令：

```
android hooking watch class_method
```

  - 事后，已知，有参数：
    - `--dump-return`
    - `--dump-args`
    - `--dump-backtrace`
  - 想要知道：
    - `android hooking watch class_method` 这个子命令
      - 是否还有其他什么参数
      - 以及这些参数的具体含义
- 目前已知：
  - `android hooking watch class_method` 这个子命令，是否还有其他什么参数
    - 可以通过tab补全，会自动列出，所有可能的参数
  - 其他子命令
    - 只有最末尾，加上 `--help` ，可以输出基本的，精简的 `help` 信息
- 效果举例
  - 无法识别的
    - 图
      - 

    - 不到末尾，输入 `--help` ，无法识别
      - 文字

```
android on (google: 13) [usb] # android hooking --help
Unknown or ambiguous command: `android hooking --help`, Try `help androi
d hooking --help`.
android on (google: 13) [usb] # android hooking generate --help
Unknown or ambiguous command: `android hooking generate --help`, Try `he
lp android hooking generate --help`.
```

- 正确用法
  - 只有最末尾，加上--help，可以输出基本的，精简的help信息

```
android on (google: 13) [usb] # android hooking watch class_method --help
Usage: android hooking watch class_method <fully qualified class method> op
tional overload> (optional: --dump-args) (optional: --dump-backtrace) (optio
nal: --dump-return)
```

  - 可以通过tab补全，会自动列出，所有可能的参数
    - 图
      - 

```
android on (google: 13) [usb] # android hooking watch class_method --help
                                                                --dump
-args
                                                                --dump
-backtrace
                                                                --dump
-return
```

crifan.org，使用署名4.0国际(CC BY 4.0)协议发布 all right reserved，powered by Gitbook最后更新：2023-09-17 01:10:14

hook函数的参数

Objection去hook安卓或iOS的函数，有些通用的逻辑

其中就包括：

- hook函数的参数
  - `--dump-args`：打印函数**参数值**
  - `--dump-backtrace`：打印函数**调用堆栈**
  - `--dump-return`：打印函数**返回值**

举例

- Android

```
android hooking watch class_method android.app.ActivityManager.forceStopPackage --d
ump-args --dump-backtrace --dump-return

android hooking watch class_method com.android.server.am.ActivityManagerService.sta
rtService --dump-args --dump-backtrace --dump-return

android hooking watch class_method jd.wjlogin_sdk.common.inland.WJLoginInland.JDLog
inWithPasswordNew --dump-args --dump-backtrace --dump-return
```

- iOS

```
ios hooking watch method "-[iGoat_Swift.BinaryCookiesExerciseVC verifyItemPressed]"
 --dump-args --dump-backtrace --dump-return
```

crifan.org，使用署名4.0国际(CC BY 4.0)协议发布 all right reserved，powered by Gitbook最后更新：2023-09-17 01:20:06

Objection调试Android

- 用Objection去调试安卓app
  - 命令

```
objection -g {androidAppPackageName} explore
```

    - 举例

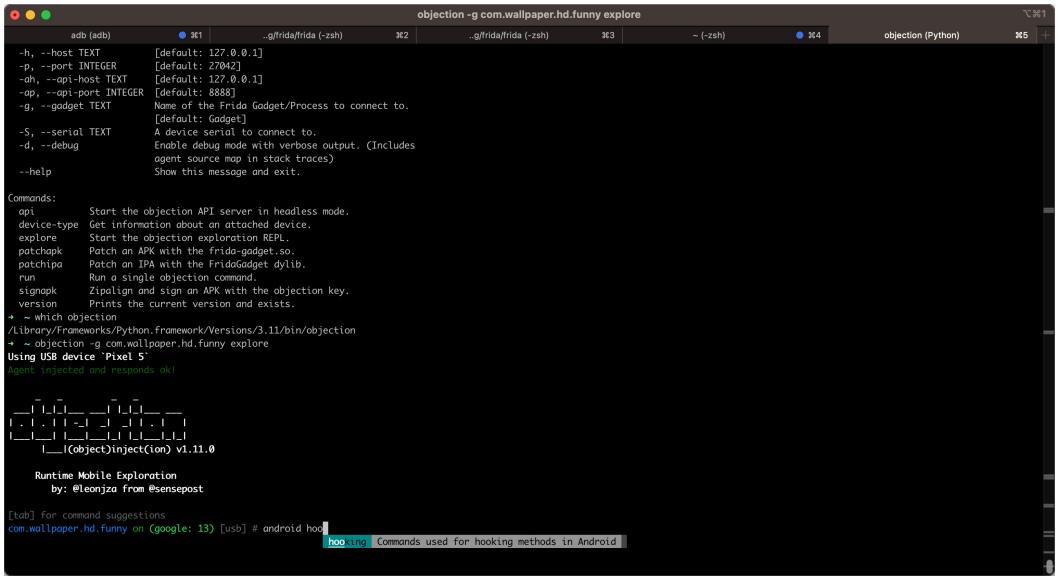
```
objection -g com.wallpaper.hd.funny explore

objection -g system_server explore
```

举例

Objection去调试360Wallpaper

- 背景
  - 被调试安卓app
    - app名称：`360Wallpaper`
    - 包名：`com.wallpaper.hd.funny`
- 命令

```
objection -g com.wallpaper.hd.funny explore
```

  - 输出效果
    - 图
      - 

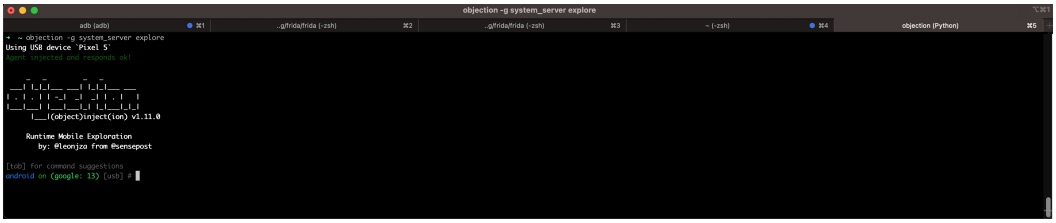
    - 文字

```
➜  ~ objection -g com.wallpaper.hd.funny explore
Using USB device `Pixel 5`
Agent injected and responds ok

     _   _ _ _____ _____   _ _ _____ _____
    | | | | |     |   __| | | |     |   | |
    | | | | |  |  |   __| | | |  |  | | | |
    |_____|_|_____|_____| |___|_____|_|___|
          |_____| (object)inject(ion) v1.11.0

    Runtime Mobile Exploration
        by: @leonjza from @sensepost

[tab] for command suggestions
com.wallpaper.hd.funny on (google: 13) [usb] #
```

Objection去调试system_server

- 命令

```
objection -g system_server explore
```

  - 输出效果
    - 图
      - 
    - 文字

```
➜  ~ objection -g system_server explore
Using USB device `Pixel 5`
Agent injected and responds ok

     _   _ _ _____ _____   _ _ _____ _____
    | | | | |     |   __| | | |     |   | |
    | | | | |  |  |   __| | | |  |  | | | |
    |_____|_|_____|_____| |___|_____|_|___|
          |_____| (object)inject(ion) v1.11.0
    Runtime Mobile Exploration
        by: @leonjza from @sensepost

[tab] for command suggestions
android on (google: 13) [usb] #
```

crifan.org，使用署名4.0国际(CC BY 4.0)协议发布 all right reserved，powered by Gitbook最后更新：2023-09-17 01:11:00

android

Objection中，对于安卓逆向的功能，都是 `android` 子命令下面的。

- 常用子命令
  - `android hooking`
  - `android intent`

crifan.org，使用署名4.0国际(CC BY 4.0)协议发布 all right reserved，powered by Gitbook最后更新：2023-09-17 00:58:41

android hooking

Objection中hook安卓一个重要的二级子命令是 `hooking` ，即： `android hooking`

- 常用子命令
  - `android hooking list`
  - `android hooking watch`
  - `android hooking search`

crifan.org，使用署名4.0国际(CC BY 4.0)协议发布 all right reserved，powered by Gitbook最后更新：2023-09-17 00:57:49

android hooking list

- 常用子命令
  - `android hooking list class_methods`
  - `android hooking list class_method`
  - `android hooking list services`
  - `android hooking list activities`
  - `android hooking list class_loaders`

crifan.org，使用署名4.0国际(CC BY 4.0)协议发布 all right reserved，powered by Gitbook最后更新：2023-09-17 01:28:21

android hooking list class_methods

Objection去hook列出单个类的所有函数 `class_methods`：

- 语法

  ```
  android hooking list class_methods {AndroidClassName}
  ```

  - 注
    - 如果不带参数，则会提示语法

      ```
      android on (google: 13) [usb] # android hooking list class_methods
      Usage: android hooking list class_methods <class name>
      ```

举例

com.example.androiddemo.Activity.FridaActivity2

- 命令

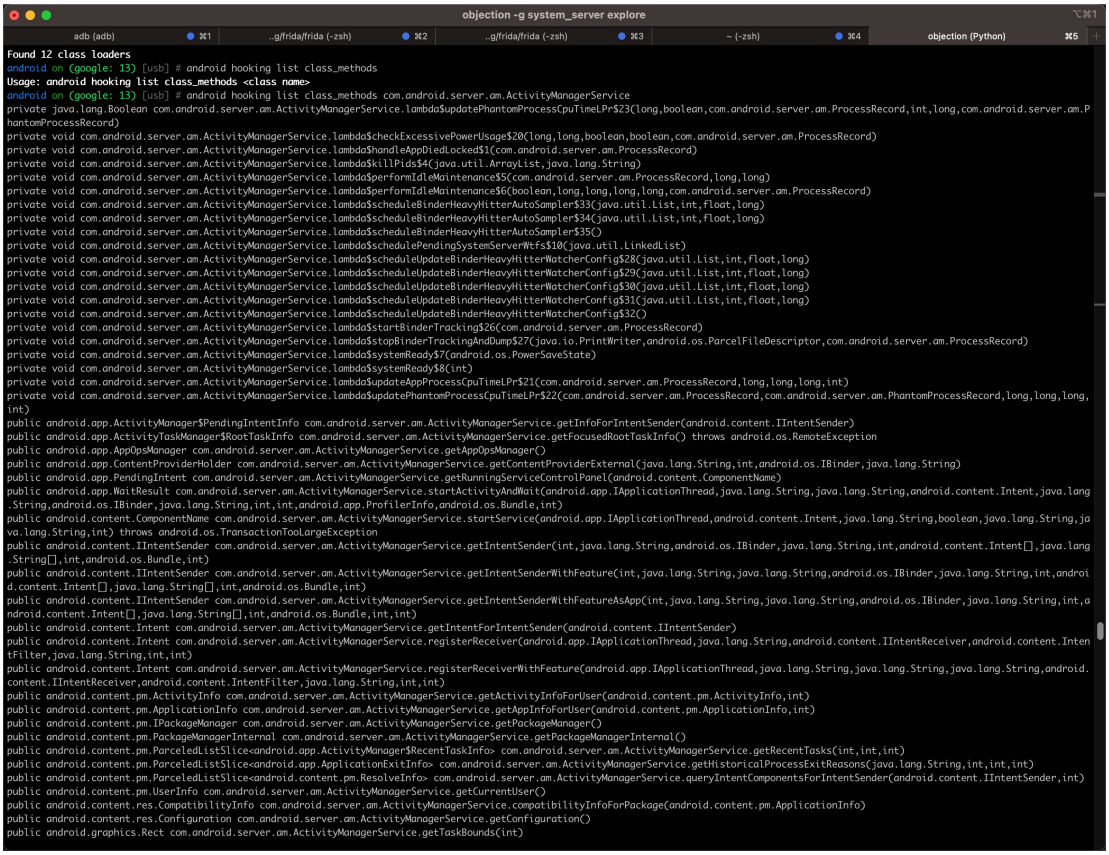
  ```
  android hooking list class_methods com.example.androiddemo.Activity.FridaActivity2
  ```

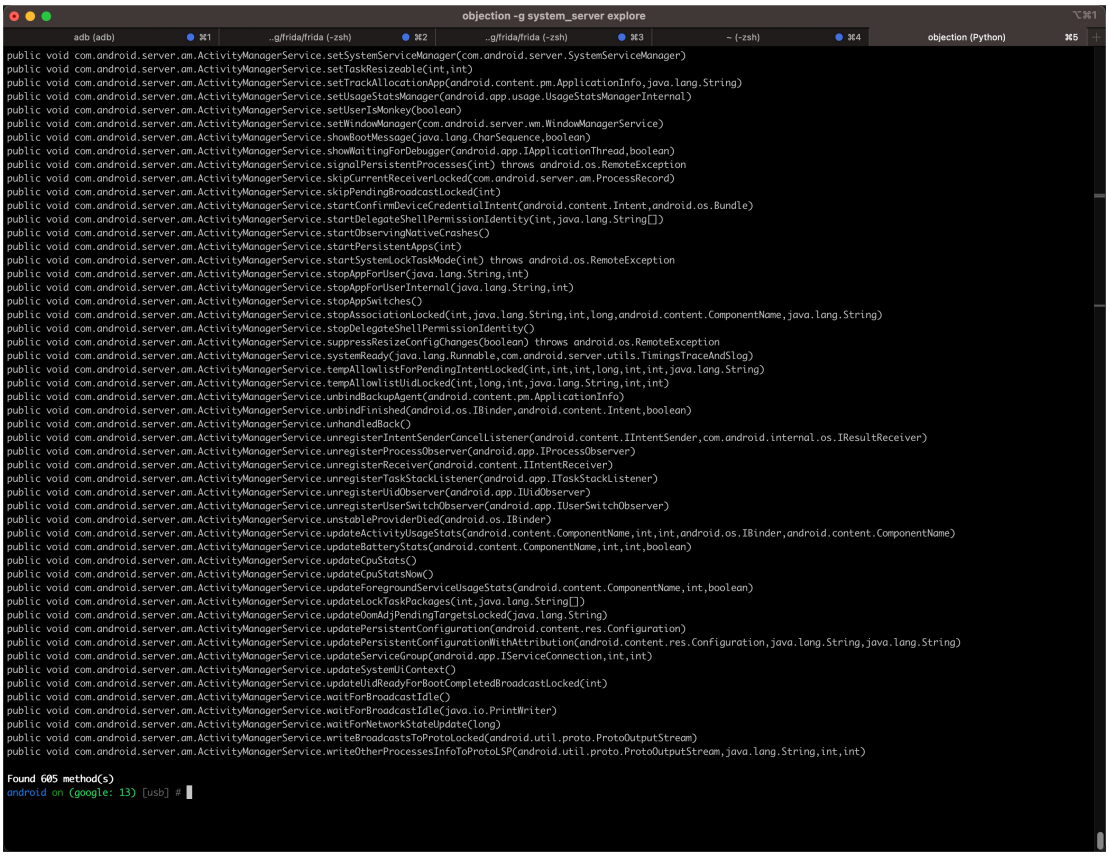
system_server

- 命令

  ```
  android hooking list class_methods com.android.server.am.ActivityManagerService
  ```

  - 图

- 

- 

- log

```
android on (google: 13) [usb] # android hooking list class_methods com.android.
server.am.ActivityManagerService
private java.lang.Boolean com.android.server.am.ActivityManagerService.lambda$u
pdatePhantomProcessCpuTimeLPr$23(long,boolean,com.android.server.am.ProcessReco
```

```
rd,int,long,com.android.server.am.PhantomProcessRecord)
private void com.android.server.am.ActivityManagerService.lambda$checkExcessive
PowerUsage$20(long,long,boolean,boolean,com.android.server.am.ProcessRecord)
private void com.android.server.am.ActivityManagerService.lambda$handleAppDiedL
ocked$1(com.android.server.am.ProcessRecord)
private void com.android.server.am.ActivityManagerService.lambda$killPids$4(jav
a.util.ArrayList,java.lang.String)
private void com.android.server.am.ActivityManagerService.lambda$performIdleMai
ntenance$5(com.android.server.am.ProcessRecord,long,long)
private void com.android.server.am.ActivityManagerService.lambda$performIdleMai
ntenance$6(boolean,long,long,long,long,com.android.server.am.ProcessRecord)
private void com.android.server.am.ActivityManagerService.lambda$scheduleBinder
HeavyHitterAutoSampler$33(java.util.List,int,float,long)
private void com.android.server.am.ActivityManagerService.lambda$scheduleBinder
HeavyHitterAutoSampler$34(java.util.List,int,float,long)
private void com.android.server.am.ActivityManagerService.lambda$scheduleBinder
HeavyHitterAutoSampler$35()
private void com.android.server.am.ActivityManagerService.lambda$schedulePendin
gSystemServerWtfs$10(java.util.LinkedList)
private void com.android.server.am.ActivityManagerService.lambda$scheduleUpdate
BinderHeavyHitterWatcherConfig$28(java.util.List,int,float,long)
private void com.android.server.am.ActivityManagerService.lambda$scheduleUpdate
BinderHeavyHitterWatcherConfig$29(java.util.List,int,float,long)
private void com.android.server.am.ActivityManagerService.lambda$scheduleUpdate
BinderHeavyHitterWatcherConfig$30(java.util.List,int,float,long)
private void com.android.server.am.ActivityManagerService.lambda$scheduleUpdate
BinderHeavyHitterWatcherConfig$31(java.util.List,int,float,long)
private void com.android.server.am.ActivityManagerService.lambda$scheduleUpdate
BinderHeavyHitterWatcherConfig$32()
private void com.android.server.am.ActivityManagerService.lambda$startBinderTra
cking$26(com.android.server.am.ProcessRecord)
private void com.android.server.am.ActivityManagerService.lambda$stopBinderTrac
kingAndDump$27(java.io.PrintWriter,android.os.ParcelFileDescriptor,com.android.
server.am.ProcessRecord)
private void com.android.server.am.ActivityManagerService.lambda$systemReady$7(
android.os.PowerSaveState)
private void com.android.server.am.ActivityManagerService.lambda$systemReady$8(
int)
...
public void com.android.server.am.ActivityManagerService.startPersistentApps(int
)
public void com.android.server.am.ActivityManagerService.startSystemLockTaskMode
(int) throws android.os.RemoteException
public void com.android.server.am.ActivityManagerService.stopAppForUser(java.la
ng.String,int)
public void com.android.server.am.ActivityManagerService.stopAppForUserInternal(
java.lang.String,int)
public void com.android.server.am.ActivityManagerService.stopAppSwitches()
public void com.android.server.am.ActivityManagerService.stopAssociationLocked(
int,java.lang.String,int,long,android.content.ComponentName,java.lang.String)
public void com.android.server.am.ActivityManagerService.stopDelegateShellPermi
ssionIdentity()
public void com.android.server.am.ActivityManagerService.suppressResizeConfigCh
anges(boolean) throws android.os.RemoteException
public void com.android.server.am.ActivityManagerService.systemReady(java.lang.
Runnable,com.android.server.utils.TimingsTraceAndSlog)
```

```
public void com.android.server.am.ActivityManagerService.tempAllowlistForPendin
gIntentLocked(int,int,int,long,int,int,java.lang.String)
public void com.android.server.am.ActivityManagerService.tempAllowlistUidLocked(
int,long,int,java.lang.String,int,int)
public void com.android.server.am.ActivityManagerService.unbindBackupAgent(andr
oid.content.pm.ApplicationInfo)
public void com.android.server.am.ActivityManagerService.unbindFinished(android
.os.IBinder,android.content.Intent,boolean)
public void com.android.server.am.ActivityManagerService.unhandledBack()
public void com.android.server.am.ActivityManagerService.unregisterIntentSender
CancelListener(android.content.IIntentSender,com.android.internal.os.IResultRec
eiver)
public void com.android.server.am.ActivityManagerService.unregisterProcessObser
ver(android.app.IProcessObserver)
public void com.android.server.am.ActivityManagerService.unregisterReceiver(and
roid.content.IIntentReceiver)
public void com.android.server.am.ActivityManagerService.unregisterTaskStackLis
tener(android.app.ITaskStackListener)
public void com.android.server.am.ActivityManagerService.unregisterUidObserver(
android.app.IUidObserver)
public void com.android.server.am.ActivityManagerService.unregisterUserSwitchOb
server(android.app.IUserSwitchObserver)
public void com.android.server.am.ActivityManagerService.unstableProviderDied(a
ndroid.os.IBinder)
public void com.android.server.am.ActivityManagerService.updateActivityUsageSta
ts(android.content.ComponentName,int,int,android.os.IBinder,android.content.Com
ponentName)
public void com.android.server.am.ActivityManagerService.updateBatteryStats(and
roid.content.ComponentName,int,int,boolean)
public void com.android.server.am.ActivityManagerService.updateCpuStats()
public void com.android.server.am.ActivityManagerService.updateCpuStatsNow()
public void com.android.server.am.ActivityManagerService.updateForegroundServic
eUsageStats(android.content.ComponentName,int,boolean)
public void com.android.server.am.ActivityManagerService.updateLockTaskPackages(
int,java.lang.String[])
public void com.android.server.am.ActivityManagerService.updateOomAdjPendingTar
getsLocked(java.lang.String)
public void com.android.server.am.ActivityManagerService.updatePersistentConfig
uration(android.content.res.Configuration)
public void com.android.server.am.ActivityManagerService.updatePersistentConfig
urationWithAttribution(android.content.res.Configuration,java.lang.String,java.
lang.String)
public void com.android.server.am.ActivityManagerService.updateServiceGroup(and
roid.app.IServiceConnection,int,int)
public void com.android.server.am.ActivityManagerService.updateSystemUiContext()

public void com.android.server.am.ActivityManagerService.updateUidReadyForBootC
ompletedBroadcastLocked(int)
public void com.android.server.am.ActivityManagerService.waitForBroadcastIdle()
public void com.android.server.am.ActivityManagerService.waitForBroadcastIdle(j
ava.io.PrintWriter)
public void com.android.server.am.ActivityManagerService.waitForNetworkStateUpd
ate(long)
public void com.android.server.am.ActivityManagerService.writeBroadcastsToProto
Locked(android.util.proto.ProtoOutputStream)
public void com.android.server.am.ActivityManagerService.writeOtherProcessesInf
```

```
oToProtoLSP(android.util.proto.ProtoOutputStream,java.lang.String,int,int)

Found 605 method(s)
android on (google: 13) [usb] #
```

crifan.org，使用署名4.0国际(CC BY 4.0)协议发布 all right reserved，powered by Gitbook最后更新：2023-09-17 01:06:59

android hooking watch class_method

Objection去hook列出单个函数 `class_method`：

- 语法

```
android hooking watch class_method {AndroidClassFunction} [optionalParameters]
```

- 举例
  - 只加函数名

```
android hooking watch class_method android.app.ActivityManager.forceStopPackage
```

  - 加上额外参数

```
android hooking watch class_method android.app.ActivityManager.forceStopPackage
 --dump-args --dump-backtrace --dump-return

android hooking watch class_method jd.wjlogin_sdk.common.inland.WJLoginInland.J
DLoginWithPasswordNew --dump-args --dump-backtrace --dump-return
```

crifan.org，使用署名4.0国际(CC BY 4.0)协议发布 all right reserved，powered by Gitbook最后更新：2023-09-17 01:17:21

android hooking list services

Objection去hook列出服务进程：

- 命令

  ```
  android hooking list services
  ```

举例

system_server

- 截图
    -
- 文字

  ```
  android on (google: 13) [usb] # android hooking list services
  android.hardware.location.GeofenceHardwareService
  android.net.ConnectivityModuleConnector$ModuleServiceConnection
  android.net.ConnectivityModuleConnector$ModuleServiceConnection
  android.service.selectiontoolbar.DefaultSelectionToolbarRenderService
  com.android.internal.infra.AbstractRemoteService$RemoteServiceConnection
  com.android.internal.infra.AbstractRemoteService$RemoteServiceConnection
  com.android.internal.infra.AbstractRemoteService$RemoteServiceConnection
  com.android.internal.infra.AbstractRemoteService$RemoteServiceConnection
  com.android.internal.infra.AbstractRemoteService$RemoteServiceConnection
  com.android.internal.infra.AbstractRemoteService$RemoteServiceConnection
  com.android.internal.infra.AbstractRemoteService$RemoteServiceConnection
  com.android.internal.infra.AbstractRemoteService$RemoteServiceConnection
  com.android.internal.infra.AbstractRemoteService$RemoteServiceConnection
  com.android.internal.infra.AbstractRemoteService$RemoteServiceConnection
  com.android.server.BinaryTransparencyService$UpdateMeasurementsJobService
  ```

```
com.android.server.MountServiceIdler
com.android.server.NetworkScoreService$ScoringServiceConnection
com.android.server.PreloadsFileCacheExpirationJobService
com.android.server.PruneInstantAppsJobService
com.android.server.SmartStorageMaintIdler
com.android.server.ZramWriteback
com.android.server.appsearch.contactsindexer.ContactsIndexerMaintenanceService
com.android.server.autofill.AutofillCompatAccessibilityService
com.android.server.autofill.RemoteAugmentedAutofillService
com.android.server.backup.FullBackupJob
com.android.server.backup.KeyValueBackupJob
com.android.server.blob.BlobStoreIdleJobService
com.android.server.bluetooth.BluetoothManagerService$BluetoothServiceConnection
com.android.server.bluetooth.BluetoothManagerService$ProfileServiceConnections
com.android.server.bluetooth.BluetoothManagerService$ProfileServiceConnections
com.android.server.bluetooth.BluetoothManagerService$ProfileServiceConnections
com.android.server.bluetooth.BluetoothManagerService$ProfileServiceConnections
com.android.server.bluetooth.BluetoothManagerService$ProfileServiceConnections
com.android.server.bluetooth.BluetoothManagerService$ProfileServiceConnections
com.android.server.bluetooth.BluetoothManagerService$ProfileServiceConnections
com.android.server.bluetooth.BluetoothManagerService$ProfileServiceConnections
com.android.server.bluetooth.BluetoothManagerService$ProfileServiceConnections
com.android.server.camera.CameraStatsJobService
com.android.server.companion.InactiveAssociationsRemovalService
com.android.server.compos.IsolatedCompilationJobService
com.android.server.content.SyncJobService
com.android.server.content.SyncManager$ActiveSyncContext
com.android.server.content.SyncManager$ActiveSyncContext
com.android.server.content.SyncManager$ActiveSyncContext
com.android.server.content.SyncManager$ActiveSyncContext
com.android.server.display.BrightnessIdleJob
com.android.server.dreams.DreamController$DreamRecord
com.android.server.inputmethod.InputMethodBindingController$2
com.android.server.job.JobServiceContext
com.android.server.job.JobServiceContext
com.android.server.job.JobServiceContext
com.android.server.job.JobServiceContext
com.android.server.job.JobServiceContext
com.android.server.location.geofence.GeofenceProxy$GeofenceProxyServiceConnection
com.android.server.net.watchlist.ReportWatchlistJobService
com.android.server.notification.ManagedServices$1
com.android.server.notification.ManagedServices$1
com.android.server.notification.ManagedServices$1
com.android.server.notification.ManagedServices$1
com.android.server.notification.ManagedServices$1
com.android.server.notification.ManagedServices$1
com.android.server.notification.ManagedServices$1
com.android.server.notification.ManagedServices$1
com.android.server.notification.NotificationHistoryJobService
com.android.server.notification.ReviewNotificationPermissionsJobService
com.android.server.people.data.DataMaintenanceService
com.android.server.pm.BackgroundDexOptJobService
com.android.server.pm.DynamicCodeLoggingService
com.android.server.pm.InstantAppResolverConnection$MyServiceConnection
com.android.server.pm.PackageManagerShellCommandDataLoader
com.android.server.policy.keyguard.KeyguardServiceDelegate$1
```

```
com.android.server.profcollect.ProfcollectForwardingService$ProfcollectBGJobService
com.android.server.servicewatcher.ServiceWatcherImpl$MyServiceConnection
com.android.server.servicewatcher.ServiceWatcherImpl$MyServiceConnection
com.android.server.servicewatcher.ServiceWatcherImpl$MyServiceConnection
com.android.server.servicewatcher.ServiceWatcherImpl$MyServiceConnection
com.android.server.servicewatcher.ServiceWatcherImpl$MyServiceConnection
com.android.server.servicewatcher.ServiceWatcherImpl$MyServiceConnection
com.android.server.storage.DiskStatsLoggingService
com.android.server.storage.StorageUserConnection$ActiveConnection$1
com.android.server.systemcaptions.RemoteSystemCaptionsManagerService$RemoteServiceC
onnection
com.android.server.telecom.TelecomLoaderService$TelecomServiceConnection
com.android.server.timezone.TimeZoneUpdateIdler
com.android.server.usage.UsageStatsIdleService
com.android.server.voiceinteraction.VoiceInteractionManagerServiceImpl$2
com.android.server.wallpaper.WallpaperManagerService$WallpaperConnection
com.android.server.wallpaper.WallpaperManagerService$WallpaperConnection

Found 87 classes
android on (google: 13) [usb] #
```

com.wallpaper.hd.funny

- 截图

- 文字

```
com.wallpaper.hd.funny on (google: 13) [usb] # android hooking list services
androidx.room.MultiInstanceInvalidationService
bk
bk
com.applovin.impl.adview.activity.FullscreenAdService
com.applovin.impl.sdk.utils.AppKilledService
com.blankj.utilcode.util.MessengerUtils$ServerService
com.bytedance.sdk.openadsdk.multipro.aidl.BinderPoolService
com.bytedance.sdk.openadsdk.multipro.aidl.a$1
com.exp.wallpaper.ser.LiveSer
com.google.android.datatransport.runtime.backends.TransportBackendDiscovery
com.google.android.datatransport.runtime.scheduling.jobscheduling.JobInfoSchedulerS
ervice
com.google.android.gms.auth.api.signin.RevocationBoundService
com.google.android.gms.measurement.AppMeasurementJobService
com.google.android.gms.measurement.AppMeasurementService
com.google.firebase.components.ComponentDiscoveryService
com.w.thsz.rev.Receiver24$a
com.w.thsz.rev.Receiver24$a
com.w.thsz.rev.Receiver24$a
com.w.thsz.rev.Receiver24$a
com.w.thsz.rev.Receiver24$a
com.w.thsz.rev.Receiver24$a
com.w.thsz.s.Service100
com.w.thsz.s.Service101
com.w.thsz.s.Service102
com.w.thsz.s.Service103
```

```
com.w.thsz.s.Service104
com.w.thsz.s.Service105
com.w.thsz.s.Service107
com.w.thsz.s.Service108
com.w.thsz.s.Service109
com.w.thsz.s.Service110
com.w.thsz.s.Service111
com.w.thsz.s.Service114
com.w.thsz.s.Service115
com.w.thsz.s.Service116
com.w.thsz.s.Service119
com.w.thsz.s.Service120
eb.a$a
eb.a$a
eb.a$a
v6.b$a
v6.b$a
v6.b$a
w.a.l.p.ser.Ser111
w.a.l.p.ser.Ser22
w.a.l.p.ser.Ser222
w.a.l.p.ser.Ser33
w.a.l.p.ser.Ser333
w.a.l.p.ser.Ser44
w.a.l.p.ser.Ser444
w.a.l.p.ser.Ser55
w.a.l.p.ser.Ser555
w.a.l.p.ser.Ser66
w.a.l.p.ser.Ser666
w.a.l.p.ser.Ser77
w.a.l.p.ser.Ser777
w.a.l.p.ser.Ser88
w.a.l.p.ser.Ser888
w.a.l.p.ser.Ser99
w.a.l.p.ser.Ser999
x6.g$a
x6.g$a
x6.g$a
x6.g$a
x6.g$a
x6.g$a

Found 66 classes
com.wallpaper.hd.funny on (google: 13) [usb] #
```

crifan.org，使用署名4.0国际(CC BY 4.0)协议发布 all right reserved，powered by Gitbook最后更新：2023-09-17 00:54:37

android hooking list activities

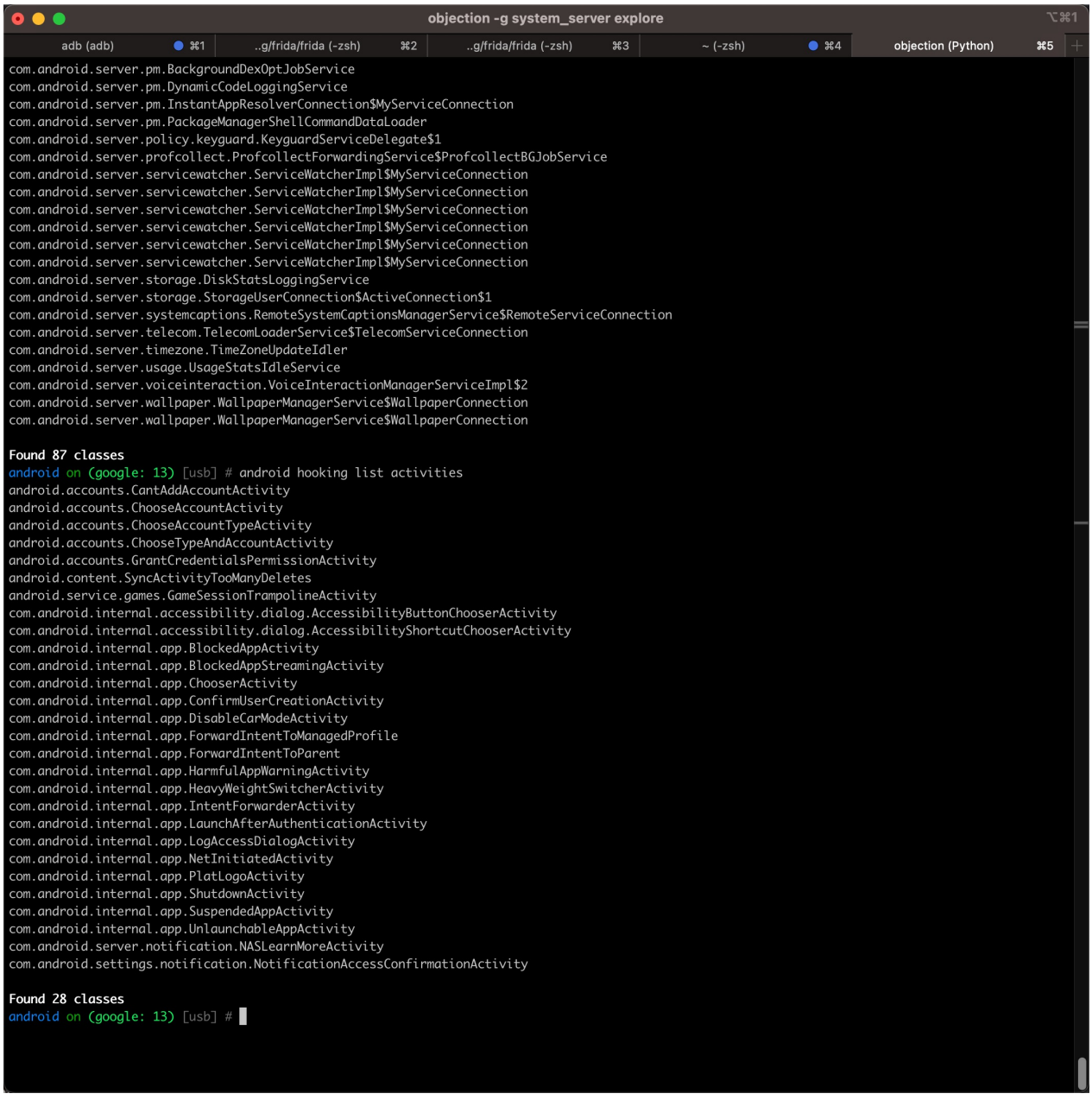
Objection去hook列出Activity页面：

- 命令

```
android hooking list activities
```

举例

system_server




```
android on (google: 13) [usb] # android hooking list activities
android.accounts.CantAddAccountActivity
```

```
android.accounts.ChooseAccountActivity
android.accounts.ChooseAccountTypeActivity
android.accounts.ChooseTypeAndAccountActivity
android.accounts.GrantCredentialsPermissionActivity
android.content.SyncActivityTooManyDeletes
android.service.games.GameSessionTrampolineActivity
com.android.internal.accessibility.dialog.AccessibilityButtonChooserActivity
com.android.internal.accessibility.dialog.AccessibilityShortcutChooserActivity
com.android.internal.app.BlockedAppActivity
com.android.internal.app.BlockedAppStreamingActivity
com.android.internal.app.ChooserActivity
com.android.internal.app.ConfirmUserCreationActivity
com.android.internal.app.DisableCarModeActivity
com.android.internal.app.ForwardIntentToManagedProfile
com.android.internal.app.ForwardIntentToParent
com.android.internal.app.HarmfulAppWarningActivity
com.android.internal.app.HeavyWeightSwitcherActivity
com.android.internal.app.IntentForwarderActivity
com.android.internal.app.LaunchAfterAuthenticationActivity
com.android.internal.app.LogAccessDialogActivity
com.android.internal.app.NetInitiatedActivity
com.android.internal.app.PlatLogoActivity
com.android.internal.app.ShutdownActivity
com.android.internal.app.SuspendedAppActivity
com.android.internal.app.UnlaunchableAppActivity
com.android.server.notification.NASLearnMoreActivity
com.android.settings.notification.NotificationAccessConfirmationActivity

Found 28 classes
```

com.example.androiddemo

```
E:\homework_python\venv\Scripts>objection -g  com.example.androiddemo explore
Checking for a newer version of objection...
Using USB device `Pixel 4`
Agent injected and responds ok!

     |___|(object)inject(ion) v1.11.0

     Runtime Mobile Exploration
        by: @leonjza from @sensepost

[tab] for command suggestions
com.example.androiddemo on (google: 11) [usb] #
com.example.androiddemo on (google: 11) [usb] #
com.example.androiddemo on (google: 11) [usb] #
com.example.androiddemo on (google: 11) [usb] # android hooking list activities
com.example.androiddemo.Activity.BaseFridaActivity
com.example.androiddemo.Activity.FridaActivity1
com.example.androiddemo.Activity.FridaActivity2
com.example.androiddemo.Activity.FridaActivity3
com.example.androiddemo.Activity.FridaActivity4
com.example.androiddemo.Activity.FridaActivity5
com.example.androiddemo.Activity.FridaActivity6
com.example.androiddemo.Activity.FridaActivity7
com.example.androiddemo.Activity.LoginActivity
com.example.androiddemo.MainActivity
```

crifan.org，使用署名4.0国际(CC BY 4.0)协议发布 all right reserved，powered by Gitbook最后更新：2023-09-17 00:55:37

android hooking list class_loaders

Objection去hook列出类加载器：

- 命令

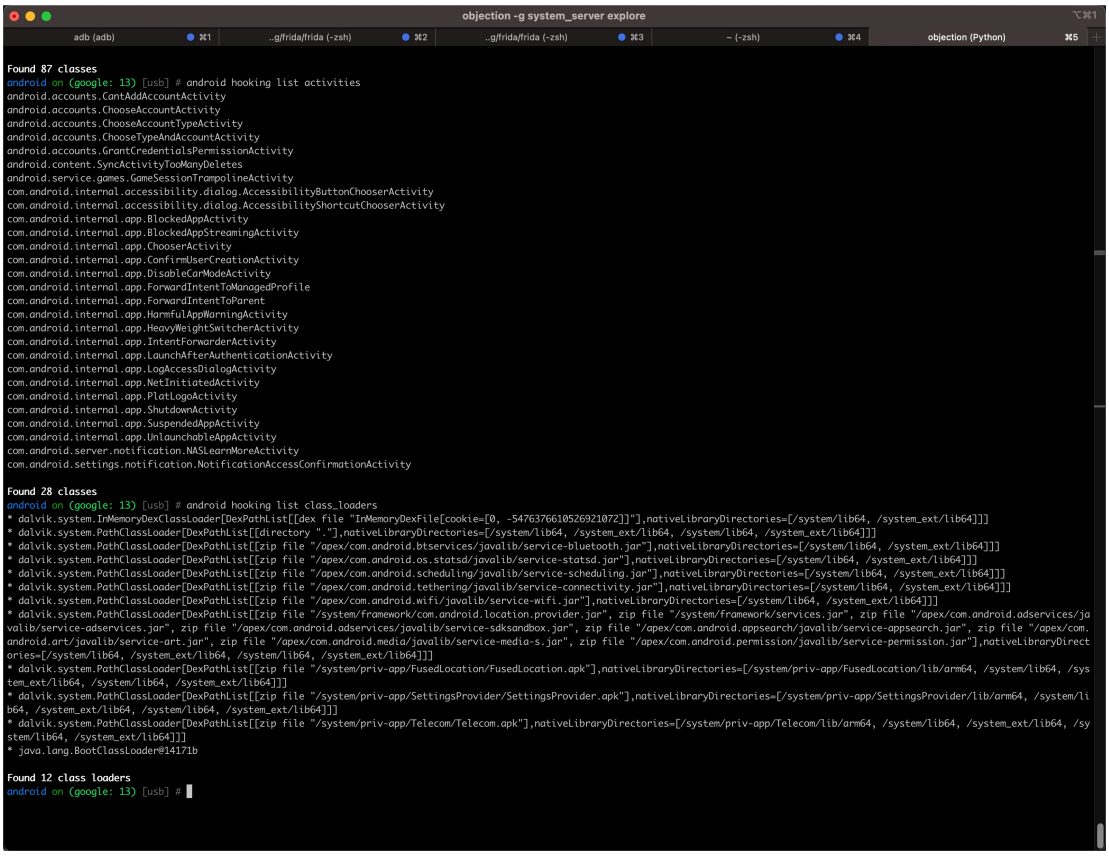
```
android hooking list class_loaders
```

举例

system_server

- 命令

```
android hooking list class_loaders
```

  - 图
    - 

  - log

```
android on (google: 13) [usb] # android hooking list class_loaders
* dalvik.system.InMemoryDexClassLoader[DexPathList[[dex file "InMemoryDexFile[cookie=[0, -5476376610526921072]]"],nativeLibraryDirectories=[/system/lib64, /system_ext/lib64]]]
* dalvik.system.PathClassLoader[DexPathList[[directory "."],nativeLibraryDirectories=[/system/lib64, /system_ext/lib64, /system/lib64, /system_ext/lib64]]]
```

```
* dalvik.system.PathClassLoader[DexPathList[[zip file "/apex/com.android.btservices/javalib/service-bluetooth.jar"],nativeLibraryDirectories=[/system/lib64, /system_ext/lib64]]]
* dalvik.system.PathClassLoader[DexPathList[[zip file "/apex/com.android.os.statsd/javalib/service-statsd.jar"],nativeLibraryDirectories=[/system/lib64, /system_ext/lib64]]]
* dalvik.system.PathClassLoader[DexPathList[[zip file "/apex/com.android.scheduling/javalib/service-scheduling.jar"],nativeLibraryDirectories=[/system/lib64, /system_ext/lib64]]]
* dalvik.system.PathClassLoader[DexPathList[[zip file "/apex/com.android.tethering/javalib/service-connectivity.jar"],nativeLibraryDirectories=[/system/lib64, /system_ext/lib64]]]
* dalvik.system.PathClassLoader[DexPathList[[zip file "/apex/com.android.wifi/javalib/service-wifi.jar"],nativeLibraryDirectories=[/system/lib64, /system_ext/lib64]]]
* dalvik.system.PathClassLoader[DexPathList[[zip file "/system/framework/com.android.location.provider.jar", zip file "/system/framework/services.jar", zip file "/apex/com.android.adservices/javalib/service-adservices.jar", zip file "/apex/com.android.adservices/javalib/service-sdksandbox.jar", zip file "/apex/com.android.appsearch/javalib/service-appsearch.jar", zip file "/apex/com.android.art/javalib/service-art.jar", zip file "/apex/com.android.media/javalib/service-media-s.jar", zip file "/apex/com.android.permission/javalib/service-permission.jar"],nativeLibraryDirectories=[/system/lib64, /system_ext/lib64, /system/lib64, /system_ext/lib64]]]
* dalvik.system.PathClassLoader[DexPathList[[zip file "/system/priv-app/FusedLocation/FusedLocation.apk"],nativeLibraryDirectories=[/system/priv-app/FusedLocation/lib/arm64, /system/lib64, /system_ext/lib64, /system/lib64, /system_ext/lib64]]]
* dalvik.system.PathClassLoader[DexPathList[[zip file "/system/priv-app/SettingsProvider/SettingsProvider.apk"],nativeLibraryDirectories=[/system/priv-app/SettingsProvider/lib/arm64, /system/lib64, /system_ext/lib64, /system/lib64, /system_ext/lib64]]]
* dalvik.system.PathClassLoader[DexPathList[[zip file "/system/priv-app/Telecom/Telecom.apk"],nativeLibraryDirectories=[/system/priv-app/Telecom/lib/arm64, /system/lib64, /system_ext/lib64, /system/lib64, /system_ext/lib64]]]
* java.lang.BootClassLoader@14171b

Found 12 class loaders
```

crifan.org，使用署名4.0国际(CC BY 4.0)协议发布 all right reserved，powered by Gitbook最后更新：2023-09-17 01:01:11

android hooking watch

hook安卓的类

- 命令

```
android hooking watch class {androidFullClassName}
```

举例

com.tlamb96.kgbmessenger.MessengerActivity

- 命令

```
android hooking watch class com.tlamb96.kgbmessenger.MessengerActivity
```

  -

asvid.github.io.fridaapp.MainActivity

- 命令

```
android hooking watch class asvid.github.io.fridaapp.MainActivity --dump-args --dum
p-return
```

-

com.example.androiddemo.Activity.LoginActivity

- 命令

```
android hooking watch class com.example.androiddemo.Activity.LoginActivity
```

-

com.example.androiddemo.Activity.FridaActivity2

- 命令

```
android hooking watch class com.example.androiddemo.Activity.FridaActivity2
```

hook安卓的函数

- 命令

```
android hooking watch class_method {androidFunctionName}
```

举例

asvid.github.io.fridaapp.MainActivity.sum

- 命令

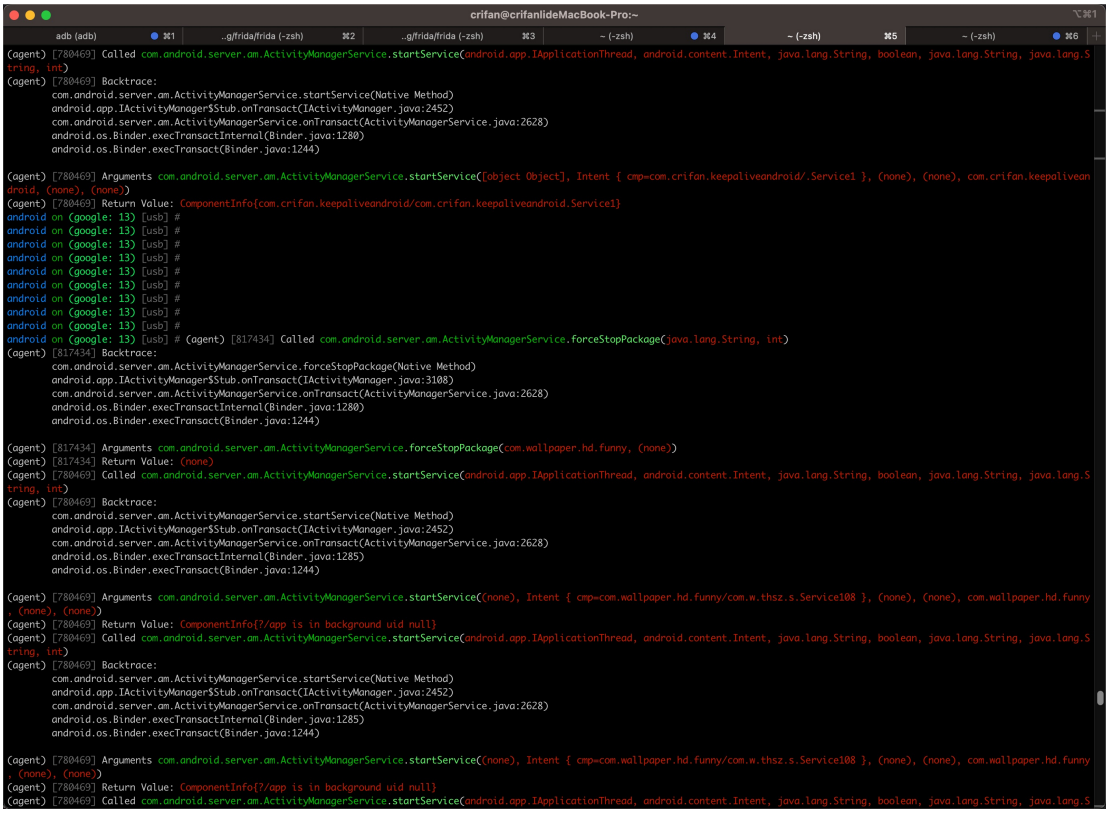
```
android hooking watch class_method asvid.github.io.fridaapp.MainActivity.sum --dump
-args --dump-backtrace --dump-return
```

com.android.server.am.ActivityManagerService.forceStopPackage

- 命令

```
android hooking watch class_method com.android.server.am.ActivityManagerService.for
ceStopPackage --dump-args --dump-backtrace --dump-return
```

  - 图



- log
  - 添加时

```
android on (google: 13) [usb] # android hooking watch class_method com.android.server.am.ActivityManagerService.forceStopPackage --dump-args --dump-backtrace --dump-return
(agent) Attempting to watch class com.android.server.am.ActivityManagerService and method forceStopPackage.
(agent) Hooking com.android.server.am.ActivityManagerService.forceStopPackage(java.lang.String, int)
(agent) Registering job 817434. Type: watch-method for: com.android.server.am.ActivityManagerService.forceStopPackage
```

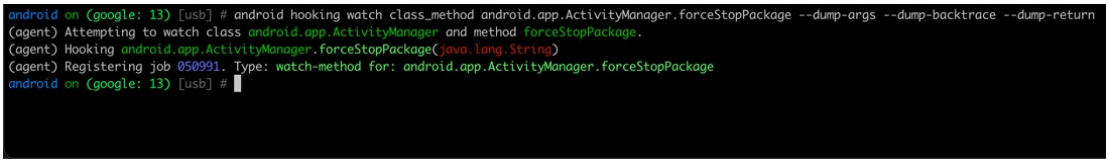
  - 触发时

```
android on (google: 13) [usb] # (agent) [817434] Called com.android.server.am.ActivityManagerService.forceStopPackage(java.lang.String, int)
(agent) [817434] Backtrace:
    com.android.server.am.ActivityManagerService.forceStopPackage(Native Method)
        android.app.IActivityManager$Stub.onTransact(IActivityManager.java:3108)
    com.android.server.am.ActivityManagerService.onTransact(ActivityManagerService.java:2628)
    android.os.Binder.execTransactInternal(Binder.java:1280)
    android.os.Binder.execTransact(Binder.java:1244)

(agent) [817434] Arguments com.android.server.am.ActivityManagerService.forceStopPackage(com.wallpaper.hd.funny, (none))
(agent) [817434] Return Value: (none)
```

android.app.ActivityManager.forceStopPackage

- 命令

```
android hooking watch class_method android.app.ActivityManager.forceStopPackage --dump-args --dump-backtrace --dump-return
```

  - 图
    - 

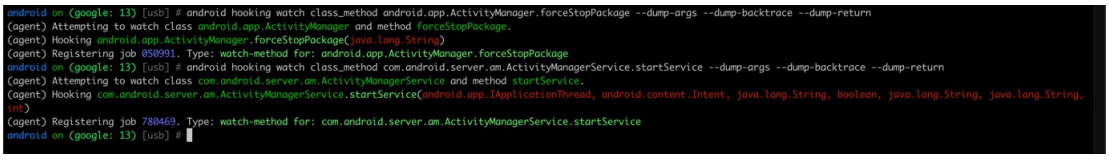
  - log

```
android on (google: 13) [usb] # android hooking watch class_method android.app.ActivityManager.forceStopPackage --dump-args --dump-backtrace --dump-return
(agent) Attempting to watch class android.app.ActivityManager and method forceStopPackage.
(agent) Hooking android.app.ActivityManager.forceStopPackage(java.lang.String)
(agent) Registering job 050991. Type: watch-method for: android.app.ActivityManager.forceStopPackage
```

com.android.server.am.ActivityManagerService.startService

- 命令

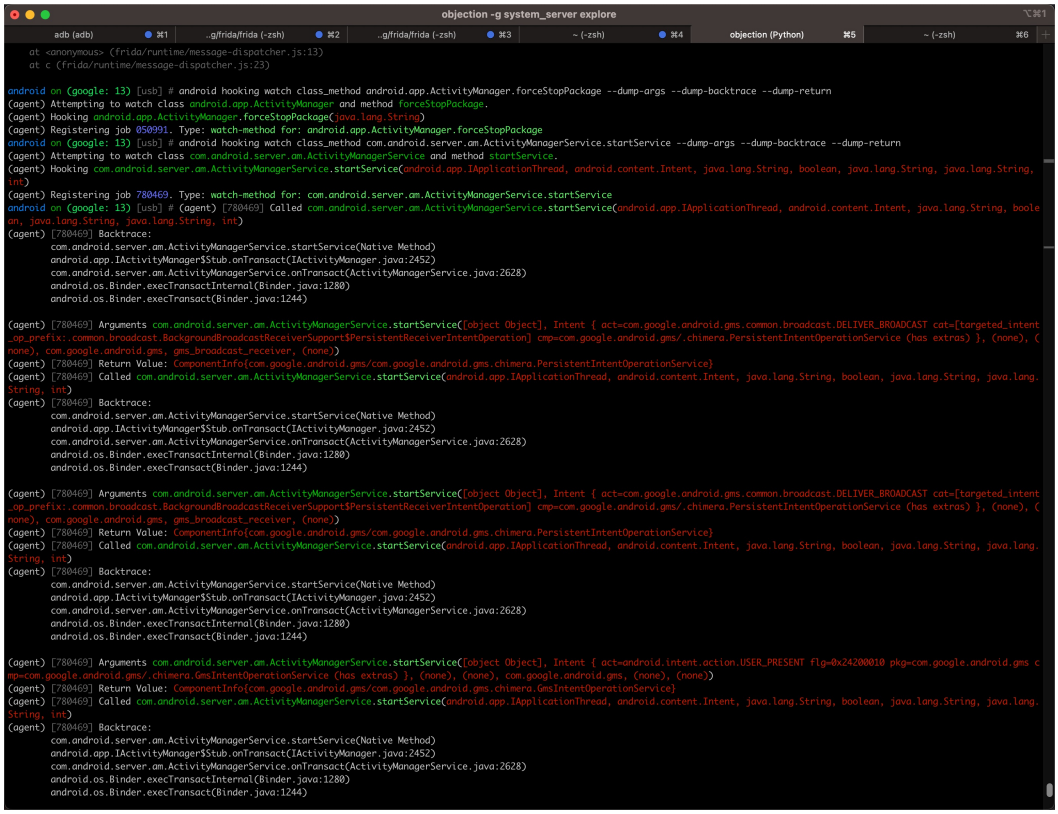
```
android hooking watch class_method com.android.server.am.ActivityManagerService.startService --dump-args --dump-backtrace --dump-return
```

  - 图
    - 

  - log

```
android on (google: 13) [usb] # android hooking watch class_method com.android.server.am.ActivityManagerService.startService --dump-args --dump-backtrace --dump-return
(agent) Attempting to watch class com.android.server.am.ActivityManagerService and method startService.
(agent) Hooking com.android.server.am.ActivityManagerService.startService(android.app.IApplicationThread, android.content.Intent, java.lang.String, boolean, java.lang.String, java.lang.String, int)
(agent) Registering job 780469. Type: watch-method for: com.android.server.am.ActivityManagerService.startService
```

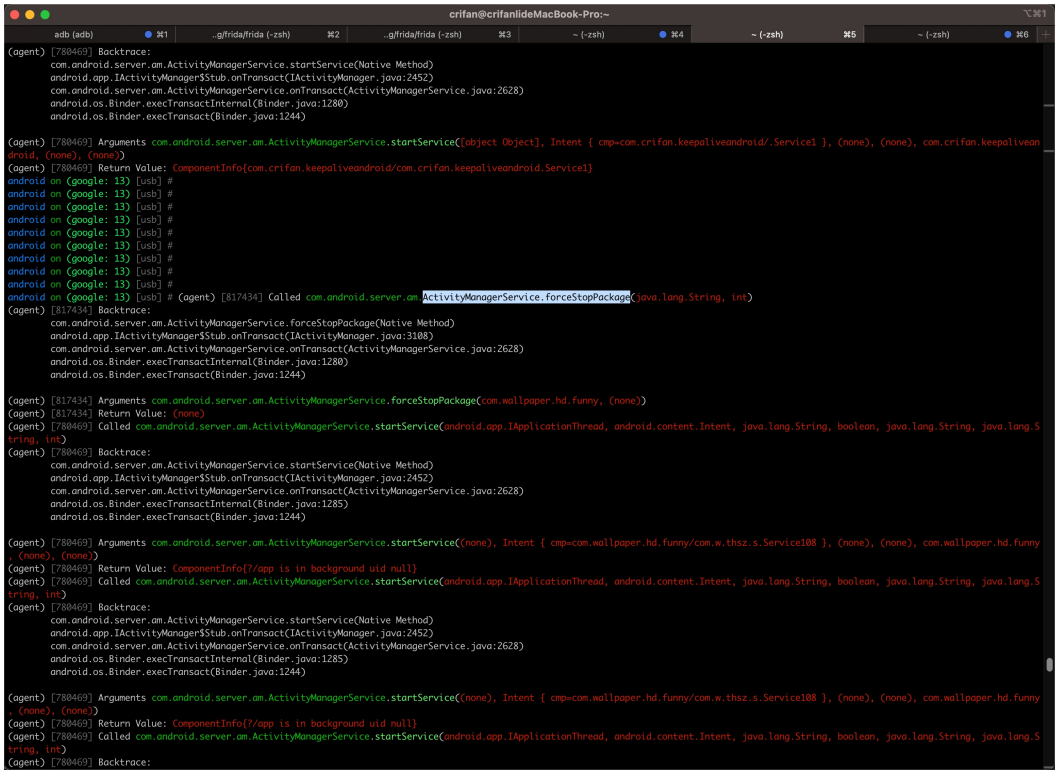
- 触发时效果
  - 效果1

- 图
  - 

- log

```
android on (google: 13) [usb] # (agent) [780469] Called com.android.server.am.ActivityManagerService.startService(android.app.IApplicationThread, android.content.Intent, java.lang.String, boolean, java.lang.String, java.lang.String, int)
(agent) [780469] Backtrace:
        com.android.server.am.ActivityManagerService.startService(Native Method)
    android.app.IActivityManager$Stub.onTransact(IActivityManager.java:2452)
    com.android.server.am.ActivityManagerService.onTransact(ActivityManagerService.java:2628)
    android.os.Binder.execTransactInternal(Binder.java:1280)
    android.os.Binder.execTransact(Binder.java:1244)

(agent) [780469] Arguments com.android.server.am.ActivityManagerService.startService([object Object], Intent { act=com.google.android.gms.common.broadcast.DELIVER_BROADCAST cat=[targeted_intent_op_prefix:.common.broadcast.BackgroundBroadcastReceiverSupport$PersistentReceiverIntentOperation] cmp=com.google.android.gms/.chimera.PersistentIntentOperationService (has extras) }, (none), (none), com.google.android.gms, gms_broadcast_receiver, (none))
(agent) [780469] Return Value: ComponentInfo{com.google.android.gms/com.google.android.gms.chimera.PersistentIntentOperationService}
(agent) [780469] Called com.android.server.am.ActivityManagerService.startService(android.app.IApplicationThread, android.content.Intent, java.lang.String, boolean, java.lang.String, java.lang.String, int)
(agent) [780469] Backtrace:
    com.android.server.am.ActivityManagerService.startService(Native Method)
    android.app.IActivityManager$Stub.onTransact(IActivityManager.java:2452)
    com.android.server.am.ActivityManagerService.onTransact(ActivityManagerService.java:2628)
```

```
    android.os.Binder.execTransactInternal(Binder.java:1280)
    android.os.Binder.execTransact(Binder.java:1244)

(agent) [780469] Arguments com.android.server.am.ActivityManagerService.star
tService([object Object], Intent { act=com.google.android.gms.common.broadca
st.DELIVER_BROADCAST cat=[targeted_intent_op_prefix:.common.broadcast.Backgr
oundBroadcastReceiverSupport$PersistentReceiverIntentOperation] cmp=com.goog
le.android.gms/.chimera.PersistentIntentOperationService (has extras) }, (no
ne), (none), com.google.android.gms, gms_broadcast_receiver, (none))
(agent) [780469] Return Value: ComponentInfo{com.google.android.gms/com.goog
le.android.gms.chimera.PersistentIntentOperationService}

...

(agent) [780469] Arguments com.android.server.am.ActivityManagerService.star
tService([object Object], Intent { act=android.intent.action.BATTERY_CHANGED
cmp=com.google.android.apps.scone/.coex.StateService (has extras) }, (none),
(none), com.google.android.apps.scone, (none), (none))
(agent) [780469] Return Value: ComponentInfo{com.google.android.apps.scone/c
om.google.android.apps.scone.coex.StateService}
(agent) [780469] Called com.android.server.am.ActivityManagerService.startSe
rvice(android.app.IApplicationThread, android.content.Intent, java.lang.Stri
ng, boolean, java.lang.String, java.lang.String, int)
(agent) [780469] Backtrace:
    com.android.server.am.ActivityManagerService.startService(Native Method)
    android.app.IActivityManager$Stub.onTransact(IActivityManager.java:2452)
    com.android.server.am.ActivityManagerService.onTransact(ActivityManagerS
ervice.java:2628)
    android.os.Binder.execTransactInternal(Binder.java:1280)
    android.os.Binder.execTransact(Binder.java:1244)

(agent) [780469] Arguments com.android.server.am.ActivityManagerService.star
tService([object Object], Intent { act=com.google.android.gms.ipa.mediastore
indexer.INSTANT_INDEX cat=[targeted_intent_op_prefix:.ipa.mediastoreindexer.
InstantIndexingIntentOperation] cmp=com.google.android.gms/.chimera.GmsInten
tOperationService (has extras) }, (none), (none), com.google.android.gms, co
m.google.android.gms.ipa, (none))
(agent) [780469] Return Value: ComponentInfo{com.google.android.gms/com.goog
le.android.gms.chimera.GmsIntentOperationService}
(agent) [780469] Called com.android.server.am.ActivityManagerService.startSe
rvice(android.app.IApplicationThread, android.content.Intent, java.lang.Stri
ng, boolean, java.lang.String, java.lang.String, int)
(agent) [780469] Backtrace:
    com.android.server.am.ActivityManagerService.startService(Native Method)
    android.app.IActivityManager$Stub.onTransact(IActivityManager.java:2452)
    com.android.server.am.ActivityManagerService.onTransact(ActivityManagerS
ervice.java:2628)
    android.os.Binder.execTransactInternal(Binder.java:1280)
    android.os.Binder.execTransact(Binder.java:1244)

(agent) [780469] Arguments com.android.server.am.ActivityManagerService.star
tService([object Object], Intent { cmp=com.crifan.keepaliveandroid/.Service1
}, (none), (none), com.crifan.keepaliveandroid, (none), (none))
(agent) [780469] Return Value: ComponentInfo{com.crifan.keepaliveandroid/com
.crifan.keepaliveandroid.Service1}
```

- 效果2
  - 图
    - 

  - log

```
(agent) [780469] Called com.android.server.am.ActivityManagerService.startSe
rvice(android.app.IApplicationThread, android.content.Intent, java.lang.Stri
ng, boolean, java.lang.String, java.lang.String, int)
(agent) [780469] Backtrace:
    com.android.server.am.ActivityManagerService.startService(Native Method)
    android.app.IActivityManager$Stub.onTransact(IActivityManager.java:2452)
    com.android.server.am.ActivityManagerService.onTransact(ActivityManagerS
ervice.java:2628)
    android.os.Binder.execTransactInternal(Binder.java:1285)
    android.os.Binder.execTransact(Binder.java:1244)
(agent) [780469] Arguments com.android.server.am.ActivityManagerService.star
tService((none), Intent { cmp=com.wallpaper.hd.funny/com.w.thsz.s.Service108
 }, (none), (none), com.wallpaper.hd.funny, (none), (none))
(agent) [780469] Return Value: ComponentInfo{?/app is in background uid null}

...
(agent) [780469] Called com.android.server.am.ActivityManagerService.startSe
rvice(android.app.IApplicationThread, android.content.Intent, java.lang.Stri
ng, boolean, java.lang.String, java.lang.String, int)
(agent) [780469] Backtrace:
    com.android.server.am.ActivityManagerService.startService(Native Method)
    android.app.IActivityManager$Stub.onTransact(IActivityManager.java:2452)
    com.android.server.am.ActivityManagerService.onTransact(ActivityManagerS
ervice.java:2628)
    android.os.Binder.execTransactInternal(Binder.java:1280)
    android.os.Binder.execTransact(Binder.java:1244)
(agent) [780469] Arguments com.android.server.am.ActivityManagerService.star
tService([object Object], Intent { cmp=com.wallpaper.hd.funny/com.w.thsz.s.S
```

```
ervice109 }, (none), (none), com.wallpaper.hd.funny, (none), (none))
(agent) [780469] Return Value: ComponentInfo{?/app is in background uid UidR
ecord{2cdc265 u0a244 TRNB idle change:procadj procs:0 seq(1409661,1409161)}}
...
(agent) [780469] Called com.android.server.am.ActivityManagerService.startSe
rvice(android.app.IApplicationThread, android.content.Intent, java.lang.Stri
ng, boolean, java.lang.String, java.lang.String, int)
(agent) [780469] Backtrace:
    com.android.server.am.ActivityManagerService.startService(Native Method)
    android.app.IActivityManager$Stub.onTransact(IActivityManager.java:2452)
    com.android.server.am.ActivityManagerService.onTransact(ActivityManagerS
ervice.java:2628)
    android.os.Binder.execTransactInternal(Binder.java:1280)
    android.os.Binder.execTransact(Binder.java:1244)
(agent) [780469] Arguments com.android.server.am.ActivityManagerService.star
tService([object Object], Intent { cmp=com.wallpaper.hd.funny/com.w.thsz.s.S
ervice111 }, (none), (none), com.wallpaper.hd.funny, (none), (none))
(agent) [780469] Return Value: ComponentInfo{?/app is in background uid UidR
ecord{2cdc265 u0a244 TRNB idle change:procadj procs:0 seq(1409838,1409161)}}
```

crifan.org，使用署名4.0国际(CC BY 4.0)协议发布 all right reserved，powered by Gitbook最后更新：2023-09-17 00:40:04

android hooking search

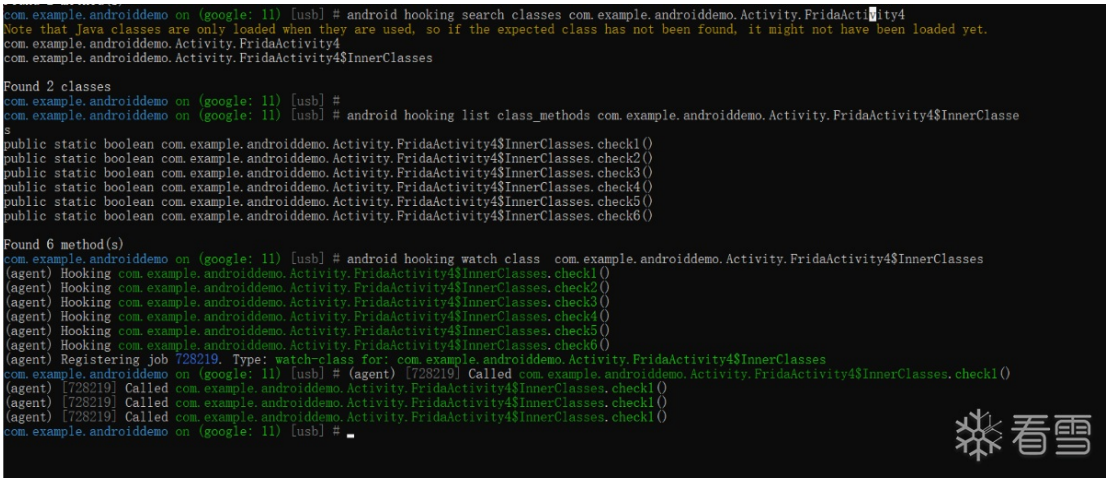
android hooking search classes

- 命令

```
android hooking search classes {AndroidClassName}
```

  - 举例

```
android hooking search classes com.example.androiddemo.Activity.FridaActivity4
```



crifan.org，使用署名4.0国际(CC BY 4.0)协议发布 all right reserved，powered by Gitbook最后更新：2023-09-17 00:08:12

android intent

- 常用子命令
  - `android intent launch_activity`

crifan.org，使用署名4.0国际(CC BY 4.0)协议发布 all right reserved，powered by Gitbook最后更新：2023-09-17 01:29:15

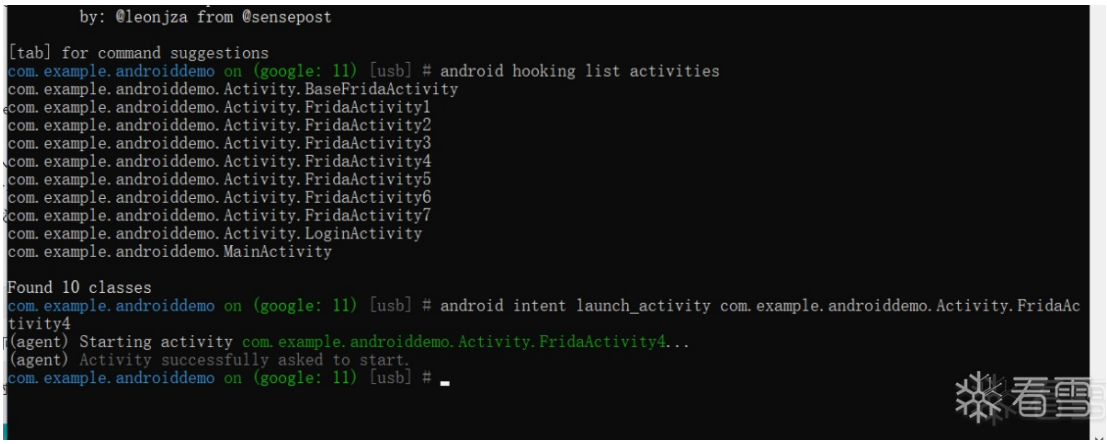
android intent launch_activity

- 命令

```
android intent launch_activity {AndroidIntentName}
```

  - 举例

```
android intent launch_activity com.example.androiddemo.Activity.FridaActivity4
```



crifan.org，使用署名4.0国际(CC BY 4.0)协议发布 all right reserved，powered by Gitbook最后更新：2023-09-17 00:08:28

memory

Objection支持内存操作，主要命令就是：`memory`

- 常用子命令
  - `memory search`
  - `memory dump`

crifan.org，使用署名4.0国际(CC BY 4.0)协议发布 all right reserved，powered by Gitbook最后更新：2023-09-17 00:59:31

memory search

Objection支持 暴力搜索内存

- 命令

```
memory search {contentToSearch}
```

  - 举例

```
memory search "64 65 78 0a 30 33 35 00"
```

crifan.org，使用署名4.0国际(CC BY 4.0)协议发布 all right reserved，powered by Gitbook最后更新：2023-09-17 00:16:22

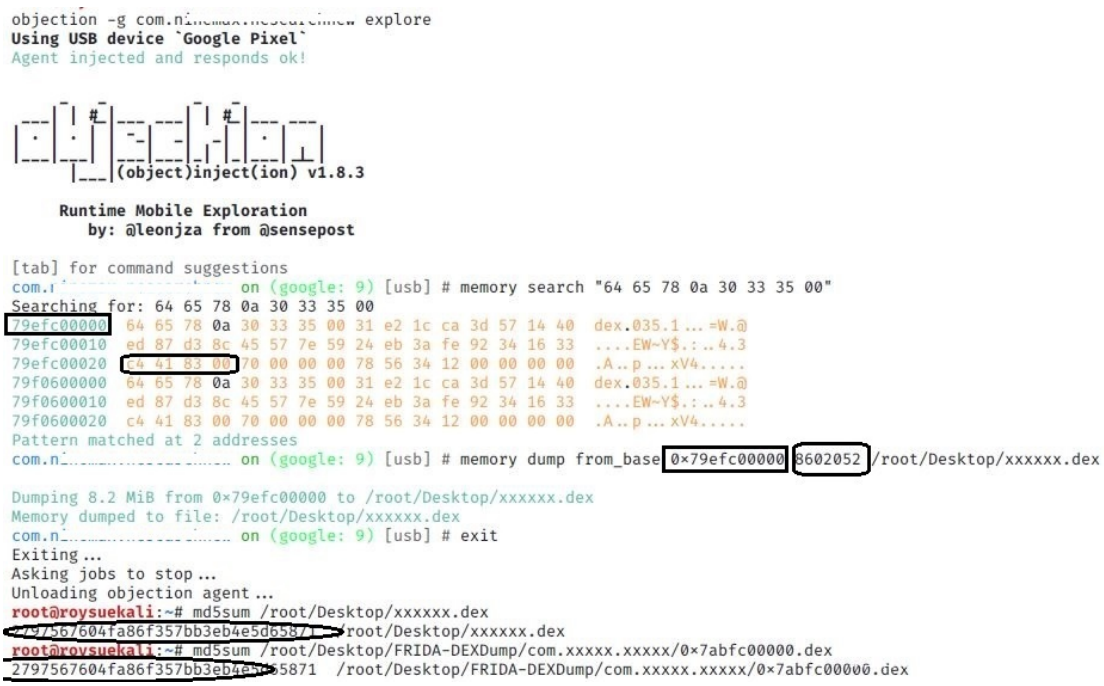
memory dump

- 命令

```
memory dump from_base {offset} {size} {outputFile}
```

  - 举例

```
memory dump from_base 0x79efc00000 8602052 /root/Desktop/xxxxxx.dex
```



crifan.org，使用署名4.0国际(CC BY 4.0)协议发布 all right reserved，powered by Gitbook最后更新：2023-09-17 00:16:40

Objection调试iOS

ios hooking watch method

- 命令

```
ios hooking watch method {iOSFullFunctionName}
```

  - 举例

```
ios hooking watch method "-[iGoat_Swift.BinaryCookiesExerciseVC verifyItemPress
ed]" --dump-args --dump-backtrace --dump-return
```

crifan.org，使用署名4.0国际(CC BY 4.0)协议发布 all right reserved，powered by Gitbook最后更新：2023-09-17 00:19:12

常见问题

crifan.org，使用署名4.0国际(CC BY 4.0)协议发布 all right reserved，powered by Gitbook最后更新：2023-09-17 01:14:30

调试安卓常见问题

hook安卓函数

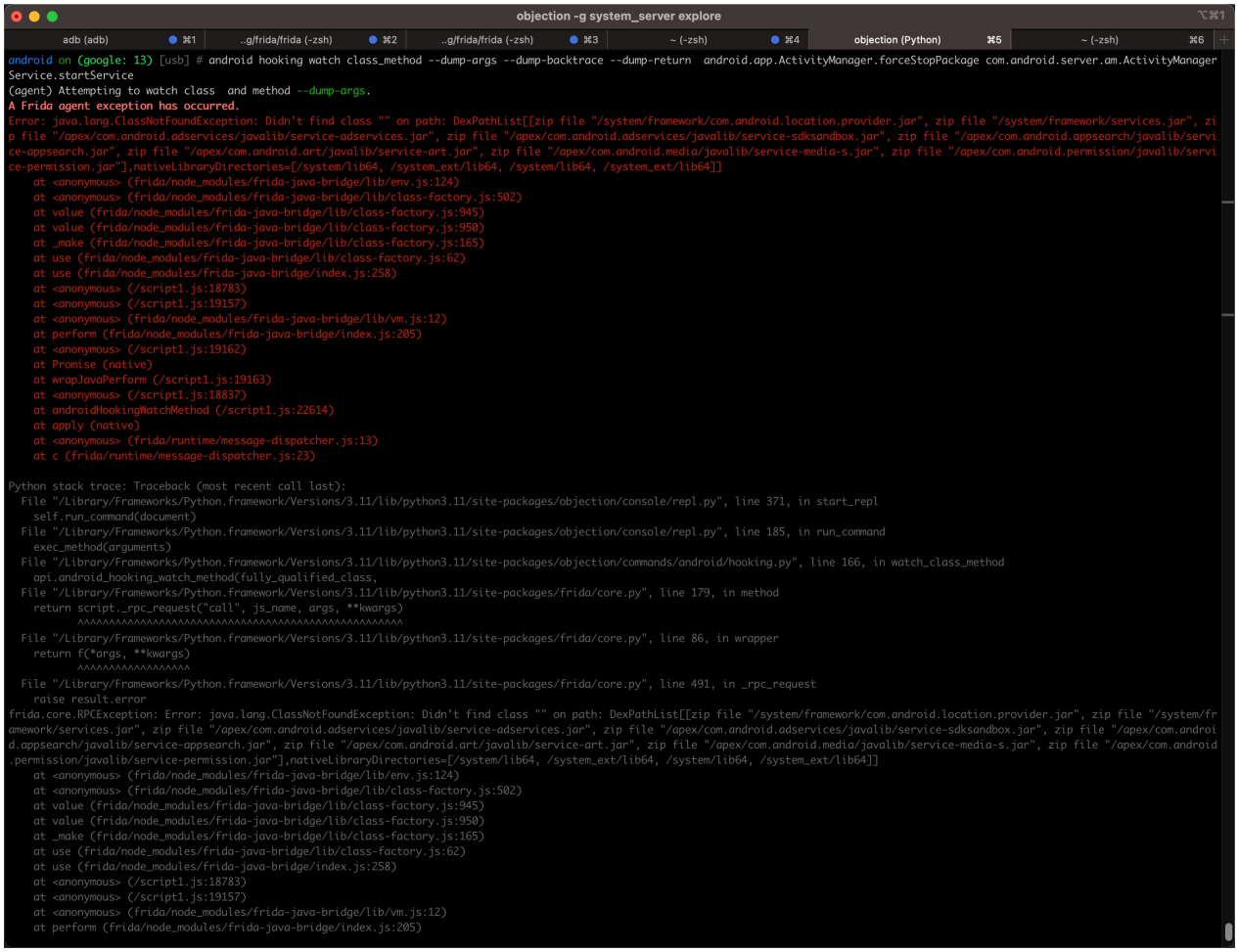
Attempting to watch class and method --dump-args A Frida agent exception has occurred

- 现象

尝试去hook安卓函数：

```
android hooking watch class_method --dump-args --dump-backtrace --dump-return  android.app.ActivityManager.forceStopPackage com.android.server.am.ActivityManagerService.startService
```

结果报错：




```
android on (google: 13) [usb] # android hooking watch class_method --dump-args --dump-backtrace --dump-return  android.app.ActivityManager.forceStopPackage com.android.server.am.ActivityManager
Service.startService
(agent) Attempting to watch class  and method --dump-args.
```

```
A Frida agent exception has occurred.
Error: java.lang.ClassNotFoundException: Didn't find class "" on path: DexPathList[[zip
file "/system/framework/com.android.location.provider.jar", zip file "/system/framework
/services.jar", zip file "/apex/com.android.adservices/javalib/service-adservices.jar",
zip file "/apex/com.android.adservices/javalib/service-sdksandbox.jar", zip file "/apex
/com.android.appsearch/javalib/service-appsearch.jar", zip file "/apex/com.android.art/
javalib/service-art.jar", zip file "/apex/com.android.media/javalib/service-media-s.jar"
, zip file "/apex/com.android.permission/javalib/service-permission.jar"],nativeLibrary
Directories [/system/lib64, /system_ext/lib64, /system/lib64, /system_ext/lib64]]
    at anonymous (frida/node_modules/frida-java-bridge/lib/env.js:124)
    at anonymous (frida/node_modules/frida-java-bridge/lib/class-factory.js:502)
    at value (frida/node_modules/frida-java-bridge/lib/class-factory.js:945)
    at value (frida/node_modules/frida-java-bridge/lib/class-factory.js:950)
    at _make (frida/node_modules/frida-java-bridge/lib/class-factory.js:165)
    at use (frida/node_modules/frida-java-bridge/lib/class-factory.js:62)
    at use (frida/node_modules/frida-java-bridge/index.js:258)
    at anonymous (/script1.js:18783)
    at anonymous (/script1.js:19157)
    at anonymous (frida/node_modules/frida-java-bridge/lib/vm.js:12)
    at perform (frida/node_modules/frida-java-bridge/index.js:205)
    at anonymous (/script1.js:19162)
    at Promise (native)
    at wrapJavaPerform (/script1.js:19163)
    at anonymous (/script1.js:18837)
    at androidHookingWatchMethod (/script1.js:22614)
    at apply (native)
    at anonymous (frida/runtime/message-dispatcher.js:13)
    at c (frida/runtime/message-dispatcher.js:23)
```

- 原因：
  - 有2处
    - 不能同时hook 2个类的函数
    - 函数的hook参数的位置方面的语法错误
      - 细节：
        - 报错信息
          - `Attempting to watch class and method --dump-args.`
          - `Error: java.lang.ClassNotFoundException: Didn't find class "" on path ...`
        - 中的
          - `class and` 的 `class` 和 `and` 中间其实有个空格 ` ` 的，其实就是表示：类名是空
          - `Didn't find class ""` 中的 `""` ，也是指的是，类名是空字符串 `""`
        - 对于类名是空字符串，当然报错找不到了
- 解决办法：
  - 单次只hook 1个函数
  - 改为正确的语法 -> 要把hook函数的 `--dump-args` 等参数，放在类的函数的最后才行
    - 详见：hook函数的参数
- 具体步骤：改为

```
android hooking watch class_method android.app.ActivityManager.forceStopPackage --d
```

```
ump-args --dump-backtrace --dump-return

android hooking watch class_method com.android.server.am.ActivityManager --dump-arg
s --dump-backtrace --dump-return
```

crifan.org，使用署名4.0国际(CC BY 4.0)协议发布 all right reserved，powered by Gitbook最后更新：2023-09-17 01:19:27

附录

下面列出相关参考资料。

crifan.org，使用署名4.0国际(CC BY 4.0)协议发布 all right reserved，powered by Gitbook最后更新：2023-09-16 22:12:24

Objection语法help

```
➜  ~ objection --help
Checking for a newer version of objection...
Usage: objection [OPTIONS] COMMAND [ARGS]...


      _   _         _   _
 ___ | |_|_|___ ___| |_|_|___ ___
| . || . | |- _|  _|  _| | . |   |
|___||___| |___|___|_| |_|___|_|_|
      |___| (object)inject(ion)


       Runtime Mobile Exploration
          by: @leonjza from @sensepost


  By default, communications will happen over USB, unless the --network option
  is provided.


Options:
  -N, --network             Connect using a network connection instead of USB.
  -h, --host TEXT           [default: 127.0.0.1]
  -p, --port INTEGER        [default: 27042]
  -ah, --api-host TEXT      [default: 127.0.0.1]
  -ap, --api-port INTEGER   [default: 8888]
  -g, --gadget TEXT         Name of the Frida Gadget/Process to connect to.
                            [default: Gadget]
  -S, --serial TEXT         A device serial to connect to.
  -d, --debug               Enable debug mode with verbose output. (Includes
                            agent source map in stack traces)
  --help                    Show this message and exit.


Commands:
  api          Start the objection API server in headless mode.
  device-type  Get information about an attached device.
  explore      Start the objection exploration REPL.
  patchapk     Patch an APK with the frida-gadget.so.
  patchipa     Patch an IPA with the FridaGadget dylib.
  run          Run a single objection command.
  signapk      Zipalign and sign an APK with the objection key.
  version      Prints the current version and exists.
```

crifan.org，使用署名4.0国际(CC BY 4.0)协议发布 all right reserved，powered by Gitbook最后更新：2023-09-16 22:22:01

Objection教程和资料

- r0ysue/AndroidSecurityStudy: 安卓应用安全学习 (github.com)
  - 内容很全的用法，值得参考
- Using objection · sensepost/objection Wiki (github.com)
  - 官网，值得继续参考试试：
    - ls
    - env
    - 等等
- 04 objection和Frida边缘化操作 - 掘金 (juejin.cn)
  - 常用命令
- 其他：
  - objection的基础使用 - 阿布_alone - 博客园 (cnblogs.com)
  - 实用FRIDA进阶：内存漫游、hook anywhere、抓包-安全客 - 安全资讯平台 (anquanke.com)

crifan.org，使用署名4.0国际(CC BY 4.0)协议发布 all right reserved，powered by Gitbook最后更新：2023-09-16 22:45:25

参考资料

- 【已解决】Mac中初始化Objection逆向安卓app的环境
- 【记录】安卓保活逆向360Wallpaper：试试Objection
- 【已解决】Objection去hook安卓函数报错：Attempting to watch class and method --dump-args A Frida agent exception has occurred
- 【已解决】Objection逆向安卓时android hooking watch class_method的--dump-return等参数的子命令的help语法说明
- 【整理】 Frida调试hook安卓：Objection使用案例
- 【已解决】安卓保活逆向研究：Objection去hook安卓forceStopPackage等函数
- 【未解决】安卓保活逆向研究：Objection调试system_server
-
- 逆向调试利器：Frida
-
- Screenshots · sensepost/objection Wiki (github.com)
- Features · sensepost/objection Wiki (github.com)
- Installation · sensepost/objection Wiki (github.com)
- Home · sensepost/objection Wiki (github.com)
- Using objection · sensepost/objection Wiki (github.com)
- Patching iOS Applications · sensepost/objection Wiki (github.com)
- Objection使用 - 简书 (jianshu.com)
- [安卓逆向]Objection的基础使用_Zeno_Lee的博客-CSDN博客
- r0ysue/AndroidSecurityStudy: 安卓应用安全学习 (github.com)
- 04 objection和Frida边缘化操作 - 掘金 (juejin.cn)
- objection的基础使用 - 阿布_alone - 博客园 (cnblogs.com)
- android逆向奇技淫巧九：frida常见java层的加密/hash算法自吐 - 第七子007 - 博客园 (cnblogs.com)
- [分享]之前大家私信我frida的一些问题，这篇文章以一些例子给大家讲一讲吧-Android安全-看雪-安全社区|安全招聘|kanxue.com
- 实用FRIDA进阶：内存漫游、hook anywhere、抓包-安全客 - 安全资讯平台 (anquanke.com)
- 实用FRIDA进阶：脱壳、自动化、高频问题-安全客 - 安全资讯平台 (anquanke.com)
- Objection使用 - 简书 (jianshu.com)
- iOS Hooking With Objection - HackTricks
- Objection Tutorial - HackTricks
- [bug] --dump-args and --dump-return not working correctly. · Issue #415 · sensepost/objection (github.com)
-

crifan.org，使用署名4.0国际(CC BY 4.0)协议发布 all right reserved，powered by Gitbook最后更新：2023-09-17 00:40:51