
目录

前言	1.1
Android逆向开发概览	1.2
Android逆向典型流程	1.3
安卓root	1.3.1
安装apk	1.3.2
搞懂逻辑	1.3.3
静态分析	1.3.3.1
动态调试	1.3.3.2
输出结果	1.3.4
重新打包apk	1.3.4.1
相关工具	1.4
相关心得	1.5
文件管理	1.5.1
文件管理器	1.5.1.1
相关资料	1.6
Android API Level	1.6.1
子教程	1.7
附录	1.8
参考资料	1.8.1

Android逆向开发

- 最新版本： `v1.5.2`
- 更新时间： `20250525`

简介

介绍Android逆向开发相关的内容。包括安卓逆向开发的典型流程图和脑图、安卓逆向的核心思路；以及Hook插件与开发，包括Xposed、Cydia Substrate，以及其插件Android-OpenDebug、Introspy-Android；以及其他心得，包括adb、文件管理、文件管理器、相关资料；以及其他相关子教程。

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/android_reverse_dev](#): Android逆向开发

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

- [Android逆向开发 book.crifan.org](#)
- [Android逆向开发 crifan.github.io](#)

离线下载阅读

- [Android逆向开发 PDF](#)
- [Android逆向开发 ePub](#)
- [Android逆向开发 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：

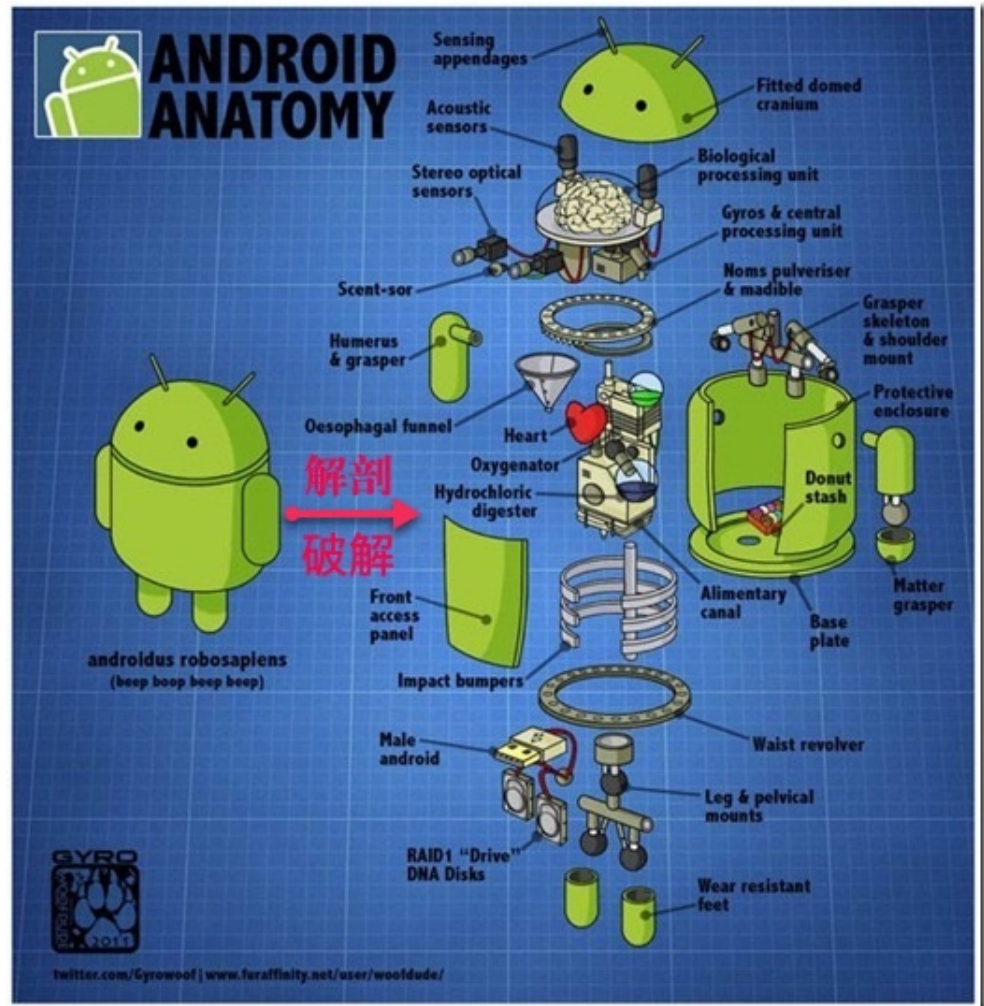
[关于CrifanLi李茂 – 在路上](#)

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：2025-04-25 16:17:53

Android逆向开发概览

此处介绍[安卓的安全和逆向](#)中的 [安卓逆向](#) 中关于 [安卓逆向开发](#) 相关的内容：

- 背景
 - 安卓应用的 存在形式
 - 静态的
 - 安装文件： apk
 - 动态的
 - 运行中的程序叫： app
 - 安卓逆向开发 = 安卓破解
 - 安卓破解 = android crack
 - 破解
 - = crack = cracking
 - 也叫 安卓逆向工程 = 安卓反向工程
 - 而逆向工程，就像对一个人去解剖



- 概述
 - 核心流程
 - 安卓root
 - 安装apk
 - 搞懂逻辑
 - 静态分析
 - 动态调试

- 输出结果
 - 重新打包apk
- 详见
 - [Android逆向典型流程](#)

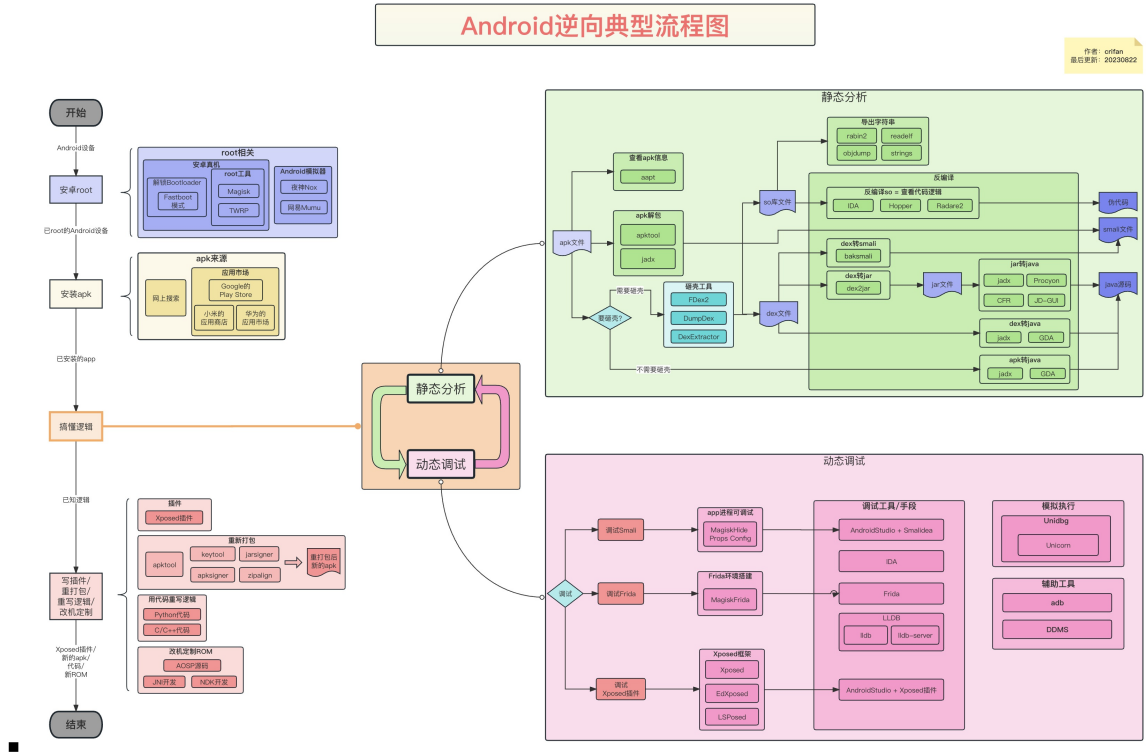
crifan.org, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新: 2023-08-30 21:10:34

Android逆向典型流程

此处整理出，安卓逆向的典型流程图和脑图：

Android逆向典型流程图

- Android逆向典型流程图
 - 在线浏览
 - Android逆向典型流程图 20230822| ProcessOn免费在线作图
 - 离线查看



Android逆向典型流程脑图

- Android逆向典型流程图
 - 在线浏览
 - Android逆向典型流程图 20230821| ProcessOn免费在线作图
 - 离线查看



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: 2023-09-13 21:29:03

安卓root

详见：

- [Android逆向：开启root](#)

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： 2024-12-06 22:05:30

安装apk

从 [应用市场](#) 或网上下载 `apk` 文件，再手动或（用 `adb` 等）自动安装安卓的apk。

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： 2024-12-06 22:06:14

搞懂逻辑

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: 2023-08-25 21:10:50

静态分析

此处主要介绍安卓的逆向破解中的静态分析：

- 安卓的逆向破解 静态分析
 - 按文件格式类型分
 - 针对 apk
 - 查看apk信息
 - aapt
 - 解包工具：输出 dex 、 so 、 smali
 - apktool
 - 反编译工具
 - 直接apk转java
 - jadx
 - JEB
 - GDA
 - 针对 dex
 - 各种导出dex的工具=砸壳工具=脱壳工具
 - FDex2
 - DumpDex
 - DexExtractor
 - 各种反编译dex的工具
 - dex转jar
 - dex2jar
 - dex转smali
 - baksmali
 - dex直接转java
 - jadx
 - GDA
 - 针对 jar
 - jar转java=各种反编译工具
 - Procyon
 - CFR
 - JD-GUI
 - 针对 so 库文件=（往往是ARM64架构）的ELF文件
 - 导出静态资源
 - readelf
 - objdump
 - razbin2
 - 反编译代码逻辑
 - IDA
 - Hopper
 - Radare2
 - Ghidra
 - 涉及子领域
 - 反代码混淆

详见独立子教程：

[Android逆向：静态分析](#)

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： 2023-09-13 21:24:34

动态调试

此处主要介绍安卓逆向破解中的动态调试：

- 安卓的逆向破解 动态调试
 - （绕过限制去）抓包
 - 绕过证书绑定的Exposed插件或Frida的脚本
 - 反root检测
 - 反反调试
 - 各种动态调试手段
 - 调试smali： `AS+smalidea`插件
 - app进程可调试
 - Magisk插件： `MagiskHide Props Config`
 - 调试Frida： `Frida`
 - Frida环境搭建
 - Magisk插件： `MagiskFrida`
 - 调试lldb： `LLDB`
 - 调试Xposed插件
 - `XPosed`
 - `EdXposed`
 - `LSPosed`
 - 模拟代码执行
 - `Unidbg`
 - `Unicorn`
 - 辅助调试工具
 - `adb`
 - `DDMS`

详见独立子教程：

[Android逆向：动态调试](#)

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： 2023-09-14 20:48:38

输出结果

此处介绍安卓的逆向破解的最终输出结果：

- 安卓的逆向破解 输出
 - 重新打包apk
 - apktool
 - keytool
 - jarsigner 或 apksigner
 - zipalign
 - 用代码重写逻辑
 - Python代码
 - C/C++代码
 - 改机定制ROM
 - AOSP源码 编译
 - JNI 开发
 - NDK 开发

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: 2023-08-25 21:13:24

重新打包apk

此处介绍安卓逆向中输出结果中的：

- 重新打包apk
 - 概述
 - apktool
 - keytool
 - jarsigner 或 apksigner
 - zipalign
 - 详解
 - [Android逆向：重新打包apk](#)

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： 2023-08-25 21:17:18

相关工具

- adb
 - 详见
 - [安卓自动化工具：adb](#)

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: 2024-12-06 22:02:25

相关心得

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: 2023-08-25 22:10:51

文件管理

TODO:

- 【记录】从Nox夜神模拟器中拷贝文件到Mac中
-
- 【已解决】 安卓手机Google Pixel3用文件管理管理文件
- 【已解决】 安卓手机中打开log日志文件查看内容

安卓逆向期间，常涉及到文件管理方面的内容。

文件上传和下载=导入导出文件

- 用文件管理器
 - 文件极客
- 用命令：`adb`
 - 概述
 - （从安卓中）导出文件

```
adb pull <remote_android> [ <local_pc> ]
```

- 导入文件（到安卓中）

```
adb push <local_pc> <remote_android>
```

- 详解
 - [安卓自动化工具](#)：`adb`

文件目录的关系

常见目录：

- `/sdcard`：SD卡根目录，即普通用户保存文件的根目录
 - `/sdcard/Download`：下载目录
 - 安卓手机中，通过 [浏览器](#) 等工具下载的文件，往往默认保存在到 `下载` 目录，就是这个：`/sdcard/Download`

对应的查看效果：

- 文件管理器
 - 文件极客
 -

3:39



下载



全部

Download

今天



EdXposed-v0.5.2.2_4683-master-z...

14.79 MB, 9分钟前



MagiskHidePropsConf-v6.1.2.zip

97.97 KB, 5小时前



昨天



magisk_patched-25200_I0hGo.img

67.11 MB, 22小时前



magisk_log_2022-09-14T17.12.35...

44.83 KB, 22小时前



8月 31, 周三



com.google.android.youtube_16.2...

101 MB, 8月31日



2009 1月 01



boot.img

67.11 MB, 2009年1月1日



- 命令行

- adb shell

```
crifan@licrifandMacBook-Pro ~/dev/dev_tool/android/EdXposed$ adb shell
blueline:/ $ whoami
shell
blueline:/ $ cd /sdcard/Download
blueline:/sdcard/Download $ ls -lh
total 120M
-rw-rw---- 1 root everybody 14M 2022-09-15 15:30 EdXposed-v0.5.2_4683-master-z-debug.zip
-rw-rw---- 1 root everybody 96K 2022-09-15 10:02 MagiskHidePropsConf-v0.1.2.zip
-rw-rw---- 1 root everybody 64M 2009-01-01 00:00 boot.img
-rw-rw---- 1 root everybody 97M 2022-08-31 11:16 com.google.android.youtube_16.29.36.apk
-rw-rw---- 1 root everybody 44K 2022-09-14 17:12 magisk_log_2022-09-14T17.12.35.log
-rw-rw---- 1 root everybody 64M 2022-09-14 17:18 magisk_patched-25200_10hGo.img
```

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: 2025-04-25 16:17:03

文件管理器

TODO:

- 【已解决】 安卓手机Google Pixel3用文件管理管理文件
- 【已解决】 安卓手机中打开log日志文件查看内容
- 【部分解决】 安卓手机Google Pixel3中用RE文件管理器拷贝和移动文件夹
- 【已解决】 导出安卓手机Google Pixel3中的文件
- 【未解决】 安卓手机Google Pixel3中用ES文件管理器拷贝和移动文件夹
- apk安装
 - 【已解决】 安卓手机中安装YouTube的apk报错：应用未安装
 - 【已解决】 安卓中把微信传输收到的apk.1改名为apk去掉.1的后缀
 - 【无需解决】 Android 9的Google Pixel3中安装apk报错应用未安装：可能和sdkVersion有关
 - 【已解决】 安卓手机Google Pixel3中用ES文件管理器安装youtube的apk
 - 【已解决】 Google Pixel3中如何彻底卸载提示未针对此用户安装的YouTube应用
 - 【已解决】 安卓手机Google Pixel3中安装apk应用
 - 【未解决】 用腾讯手机管家的APK安装器安装安卓apk应用

-
- Android的文件管理器
 - 推荐： [文件管理](#)
 - 应用宝中搜 [文件管理](#) ， 而找到的
 -

5:29 99%

文件管理

官方

文件文件管理器文件压缩文件解压

文件服务

文件管理

★ 3.8

82人评分

3255.8万
下载量

详情

评价¹²

文件智能分类

手机文件智能分类便于管理

文件编辑管理

手机所有文件多种编辑状态

微信文件管理

微信及QQ的文件分类管理

文档

手机文档管理

软件介绍

版本号 1.2.2

文件、文件管理器、文件分类、文件压缩、文件解压

文本，图片，音乐，视频，多功能与一身。

移动、排序、新建、备份，都能满足你。

文件●功能齐全，涵盖全面的文件操作

46.4%

<

>

- 其他可选
 - ES文件管理器
 - RE
 - MT管理器
 - 安卓模拟器中的文件管理器
 - 夜神模拟器中自带文件浏览器
- 常见的用途
 - 给文件改名
 - `xxx.apk.1 -> xxx.apk`
 - 查找文件
 - 再去安装apk文件
 - 查看文件内容
 - 查看log日志内容

MT管理器

- `MT = MT管理器 = MT Manager = MT Manager for Android`
- 是什么：安卓中的一个文件管理器
- 常被简称为：`MT2`
 - 因为最新版本是v2
 - 比如：
 - MT浏览器_V2.5.4.apk 文件管理器
 - 文件管理神器 MT Manager v2.6.1 for Android
 - MT管理器2.0

特点

- 支持在VirtualXposed中使用MT
- 除了普通文件管理功能外，还支持APK反编译相关功能

应用简介

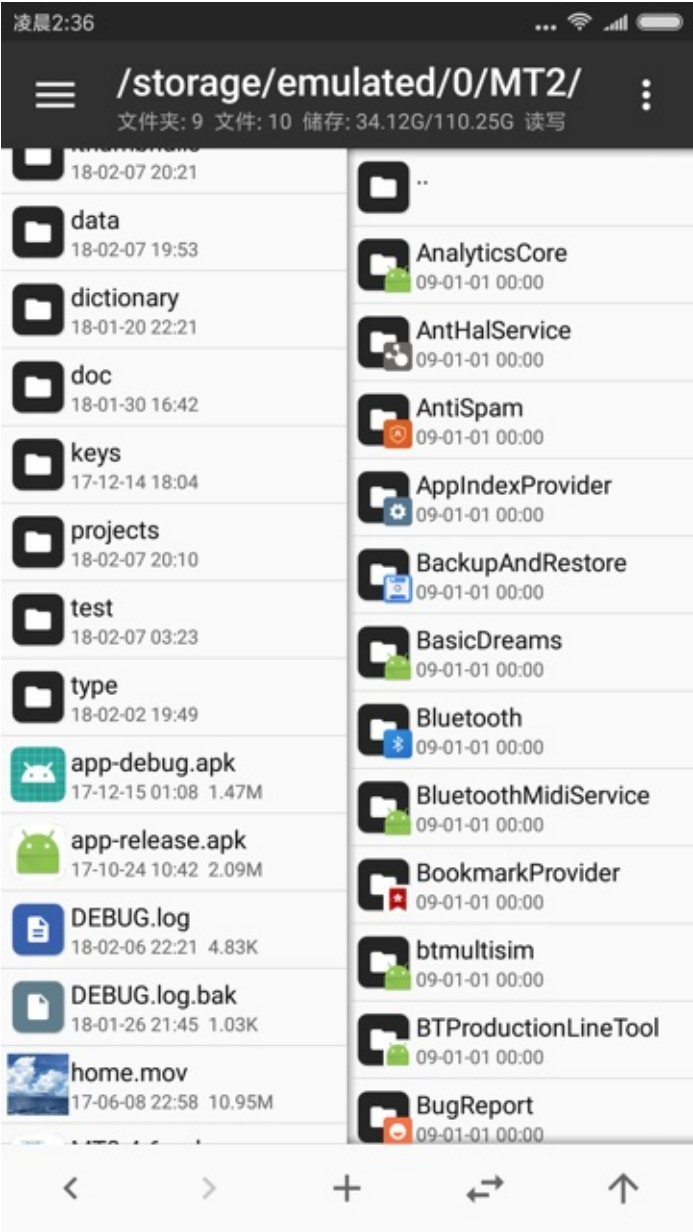
MT管理器是一款强大的文件管理工具和APK逆向修改神器。

- 如果你喜欢它的双窗口操作风格，可以单纯地把它当成文件管理器使用。
- 如果你对修改APK有深厚的兴趣，那么你可以用它做许多许多的事
 - 例如汉化应用、替换资源、修改布局、修改逻辑代码、资源混淆、去除签名校验等，主要取决于你如何使用。

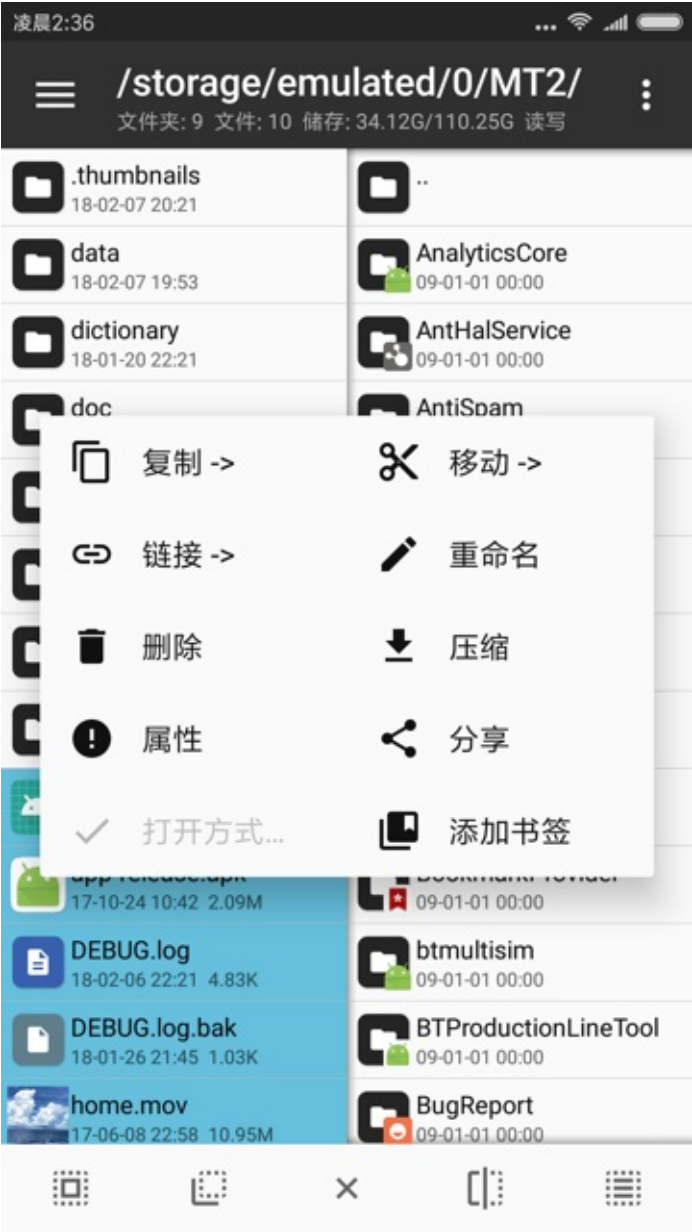
主要功能

- 文件复制、移动、创建软链接、重命名、删除、创建文件(夹)，文件批量操作。获取 Root 权限后可访问系统目录，挂载文件系统为读写，修改文件权限和所有者。
- 像 WinRAR 那样打开 ZIP 格式文件，可以对 ZIP 内的文件进行删除、重命名、移动，添加/替换外部文件到 ZIP 中，无需解压后再重新打包，同时支持单独解压 ZIP 内的部分文件。
- 自带强大的文本编辑器，可以流畅编辑大文本文件，支持设置是否显示行号、开关自动换行、双指缩放字体大小、自动识别编码、代码语法高亮、自动缩进、正则搜索替换。
- 拥有图片查看、音乐播放、字体预览、执行脚本、文本对比等功能，在侧拉栏中可方便地查看存储设备、FTP连接、书签、后台、工具等。
- APK 编辑功能，主要有 DEX 编辑，ARSC 编辑，XML 编辑，APK 签名、APK 优化、APK 共存、去除签名校验、RES 资源混淆、RES 反资源混淆、翻译模式等。

截图举例

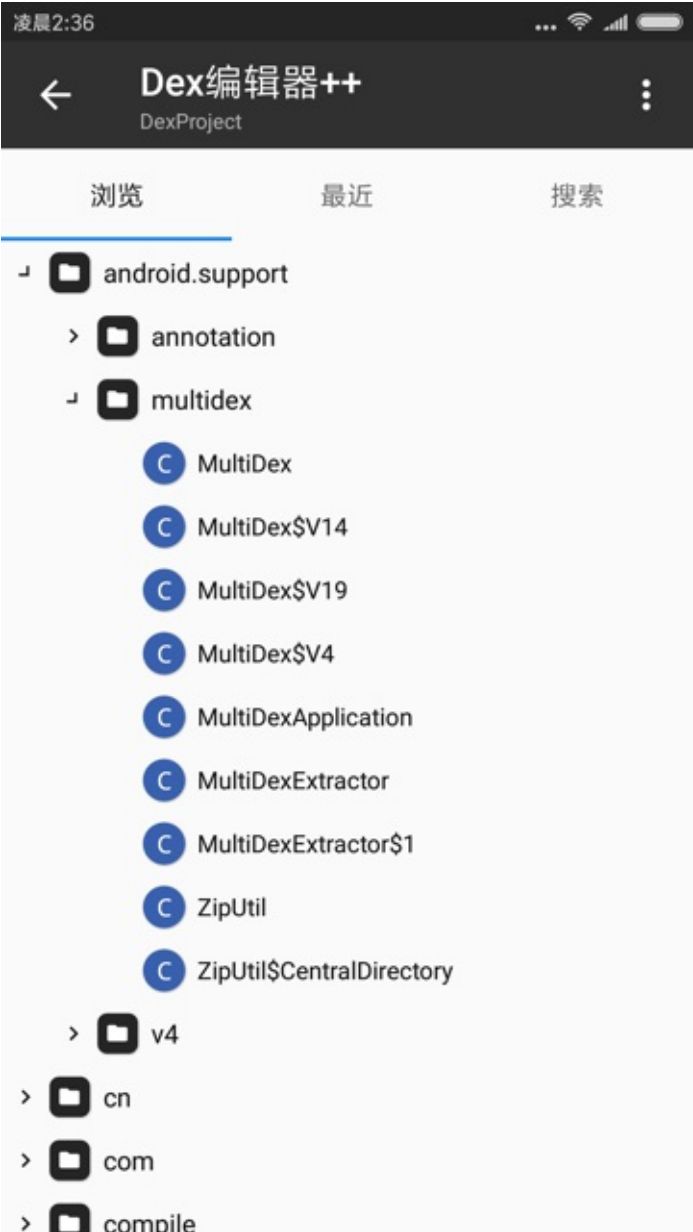












相关资料

- DDMS
 - [Using Dalvik Debug Monitor Service \(DDMS\) | Android Developers \(sourceforge.net\)](#)
 - [Using DDMS | Android Developers \(android-doc.github.io\)](#)
- 常见安卓模拟器的调试端口

-
- <https://developer.android.com>
 - 安卓 调试 debug
 - [调试应用 | Android 开发者 | Android Developers](#)

- Android Device Monitor
 - [Android Device Monitor](#) | [Android 开发者](#) | [Android Developers](#)

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: 2023-09-13 21:30:01

Android API Level

Android的 API Level 、 sdkVersion

API Levels | Android versions, SDK/API levels, version codes, codenames, and cumulative usage

https://apilevels.com

Android API Levels

This is an overview of all Android versions and their corresponding identifiers for Android developers. Anyone is welcome to open an issue or pull request. Happy developing!

Definitions Footnotes See also

Version	SDK / API level	Version code	Codename	Cumulative usage ¹	Year
Android 13	Level 33	TIRAMISU	Tiramisu ²	No data	2022
Android 12	Level 32 Android 12L	S_V2	Snow Cone ²	20.7%	2021
	Level 31 Android 12	S			
	- targetSdk must be 31+ for new apps. - targetSdk will need to be 31+ for app updates by Nov 2022 and all existing apps by Nov 2023. ³				
Android 11	Level 30	R	Red Velvet Cake ²	50.3%	2020
	- targetSdk must be 30+ for app updates, and new WearOS apps. - targetSdk will need to be 30+ for all existing apps by November 2022. ³				
Android 10	Level 29	Q	Quince Tart ²	72.1%	2019
Android 9	Level 28	P	Pie	82.9%	2018
	targetSdk must be 28+ for Wear OS app updates.				
Android 8	Level 27 Android 8.1	0_MR1	Oreo	88.4%	2017
	Level 26 Android 8.0	0		91.1%	
Android 7	Level 25 Android 7.1	N_MR1	Nougat	92.5%	2016
	Level 24 Android 7.0	N		95.1%	
Android 6	Level 23	M	Marshmallow	97.4%	2015
Android 5	Level 22 Android 5.1	LOLLIPOP_MR1	Lollipop	98.8%	2015
	Level 21 Android 5.0	LOLLIPOP, L		No data	2014
	Jetpack Compose requires a minSdk of 21 or higher.				
Android 4	Level 20 Android 4.4W ⁴	KITKAT_WATCH	KitKat		

Definitions

Gradle files

Kotlin variable	Groovy variable	Definition
<code>minSdk</code>	<code>minSdkVersion</code>	The minimum SDK version your app will support, defined in <code>build.gradle</code> . For

子教程

- 父教程
 - [安卓应用的安全和破解](#)
- 子教程
 - 通用
 - 可执行文件格式
 - [可执行文件格式：ELF](#)
 - 调试
 - [逆向调试利器：Frida](#)
 - [Frida逆向实例和工具函数](#)
 - [移动端调试利器：Objection](#)
 - [主流调试器：LLDB](#)
 - 逆向
 - [Android逆向开发](#)
 - [Android逆向：开启root](#)
 - [Android逆向：静态分析](#)
 - [安卓逆向利器：JEB](#)
 - [安卓反编译利器：jadx](#)
 - [Android逆向：动态调试](#)
 - [安卓逆向调试：Xposed框架](#)
 - [Android逆向：重新打包apk](#)
 - 相关
 - 代码
 - [Xposed插件模板演示项目](#)
 - <https://github.com/crifan/CrifanXposedHook>
 - [安卓逆向动态调试Smali示例项目：YouTube](#)
 - <https://github.com/crifan/AndroidYouTubeDynamicDebug>
 - [安卓保活演示项目](#)
 - <https://github.com/crifan/KeepAliveAndroid>
 - 工具
 - [安卓自动化工具：adb](#)
 - [安卓模拟器](#)
 - [好用的安卓模拟器：夜神Nox](#)
 - [【整理Book】流畅的安卓模拟器：网易Mumu](#)
 - 子领域
 - [安卓逆向：Root环境检测及绕过](#)
 - [安卓保活技术](#)
 - 正向开发
 - [Android开发总结](#)

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： 2025-01-23 22:53:08

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: 2022-10-27 16:42:54

参考资料

- YouTube 安卓逆向 逆向思路
- 【整理】安卓逆向：相关资料
- 【整理】安卓逆向：开发心得
-
- [Android逆向：重新打包apk](#)
- [Android逆向：静态分析](#)
-
- [Creating a URL \(The Java™ Tutorials > Custom Networking > Working with URLs\) \(oracle.com\)](#)
- [Java URL class- javatpoint](#)
- [A Simple Guide to the Java URL | Baeldung](#)
- [java - Create URL from a String - Stack Overflow](#)
- [Android逆向破解：使用Android Studio调试反编译后的smali代码 - 简书 \(jianshu.com\)](#)
- [什么刷机软件最好用\(oppo手机用什么刷机软件好用\) - 52FMZ资讯网](#)
-

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: 2024-12-06 22:03:26