跟肉丝姐学 Frida 之 快速搭建 Frida 安卓逆向环境

原创

咸鱼学 Python 于 2020-05-30 23:08:27 发布

快速搭建 Frida 安卓逆向环境

这段时间空闲的时间一直在跟着肉丝姐补课，手残把手机搞崩了，借着这个机会写一篇文章记录下如何从零完成 Frida 安卓逆向环境的搭建。

按照肉丝姐的教程，非常顺利的完成了`pixel+ andriod 8.1.0 + twrp3.3 + Magisk + Frida`这套环境的搭建，这个过程中需要的工具有：

一台 pixel 手机

一台电脑（用来开虚拟机）

所有的工具包下载地址参考肉丝姐的 Github ：
https://github.com/r0ysue/AndroidSecurityStudy/blob/master/FRIDA/A01/README.md

准备好这些工具以及相关的软件包之后开始刷机。

相关的软件放在后台，后台回复`20200530`获取。

一、快速刷机

1、检查手机确保电量充足后关机

2、 关机后按住手机的电源键和音量-键，进入`fastboot`模式（这个动作必须娴熟，之后经常用到）

3、将 `sailfish-opm1.171019.011-factory-56d15350`这个压缩包解压，可以看到有下面这些文件

4、运行 `flash-all.sh`这个文件

```
./flash-all.sh
```

5、这个过程会比较漫长，不需要做其他操作只要静静等待手机重启就可以了。

```
root@roysue:~/Desktop/sailfish-opm1.171019.011# ./flash-all.sh
Sending 'bootloader_b' (32248 KB)                  OKAY [  3.604s]
Writing 'bootloader_b'                             (bootloader) Valid bootloader version.
(bootloader) Flashing active slot "_b"
(bootloader) Flashing active slot "_b"
OKAY [ 10.214s]
Finished. Total time: 13.979s
Rebooting into bootloader                          OKAY [  0.043s]
Finished. Total time: 0.093s
Sending 'radio_b' (57320 KB)                       OKAY [  6.497s]
Writing 'radio_b'                                  OKAY [  0.903s]
Finished. Total time: 7.598s
Rebooting into bootloader                          OKAY [  0.044s]
Finished. Total time: 0.094s
----------------------------------------
Bootloader Version...: 8996-012001-1710040120
Baseband Version.....: 8996-130091-1710201747
Serial Number........: FA69P0300560
----------------------------------------
extracting android-info.txt (0 MB) to RAM...
Checking 'product'                                 OKAY [  0.049s]
Checking 'version-bootloader'                      OKAY [  0.050s]
Checking 'version-baseband'                        OKAY [  0.050s]
Setting current slot to 'b'                        OKAY [  0.409s]
extracting boot.img (28 MB) to disk... took 0.289s
archive does not contain 'boot.sig'
Sending 'boot_b' (28945 KB)                        OKAY [  3.353s]
Writing 'boot_b'                                   OKAY [  0.659s]
archive does not contain 'dtbo.img'
archive does not contain 'dt.img'
archive does not contain 'recovery.img'
archive does not contain 'vbmeta.img'
archive does not contain 'vbmeta_system.img'
archive does not contain 'vendor_boot.img'
archive does not contain 'super_empty.img'
archive does not contain 'boot_other.img'
```

6、 手机开机完成后按照下面的操作路径验证

```
手机打开设置 - 系统 - 关于手机 - Android 版本 # 版本为 8.1.0 为刷机完成
```

二、安装 twrp recovery

0、关于 `twrp` 的介绍参考肉丝姐 Github 上的内容，同时这里需要准备两个安装包

> `recovery`相当于`Windows PE`微型系统，在`recovery`里我们也可以挂载磁盘，修改系统分区，使用`adb`命令，等一系列功能。

```
twrp-pixel-installer-sailfish-3.3.0-0.zip
twrp-3.3.0-0-sailfish.img
```

1、使用下面的命令将第一个`zip`包`push`到手机的`/sdcard`下

```
adb push /yourpath/twrp-pixel-installer-sailfish-3.3.0-0.zip /sdcard
```

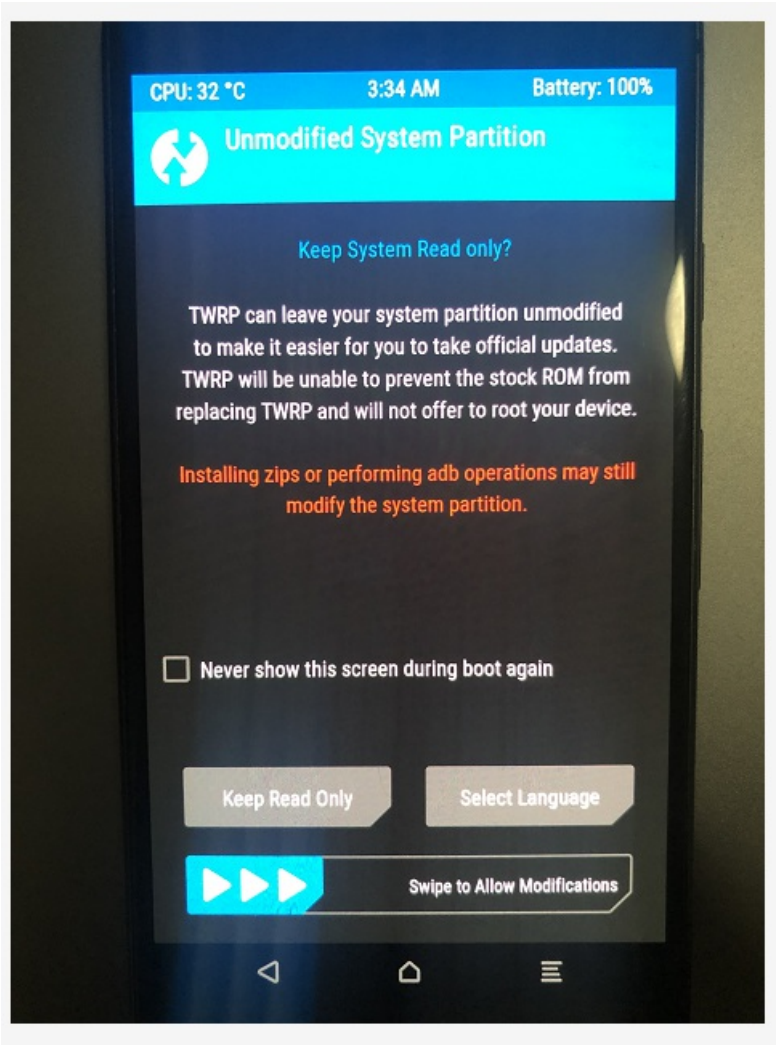
```
C:\Users\Administrator>adb push F:\App逆向资料\安卓应用安全进阶\刷机-1\twrp-pixel-installer-sailfish-3.3.0-0.zip /sdcard/
2029 KB/s (11763702 bytes in 5.659s)

C:\Users\Administrator>
```

2、push完成后，再次让手机进入到fastboot模式，使用下面的命令开始刷入twrp

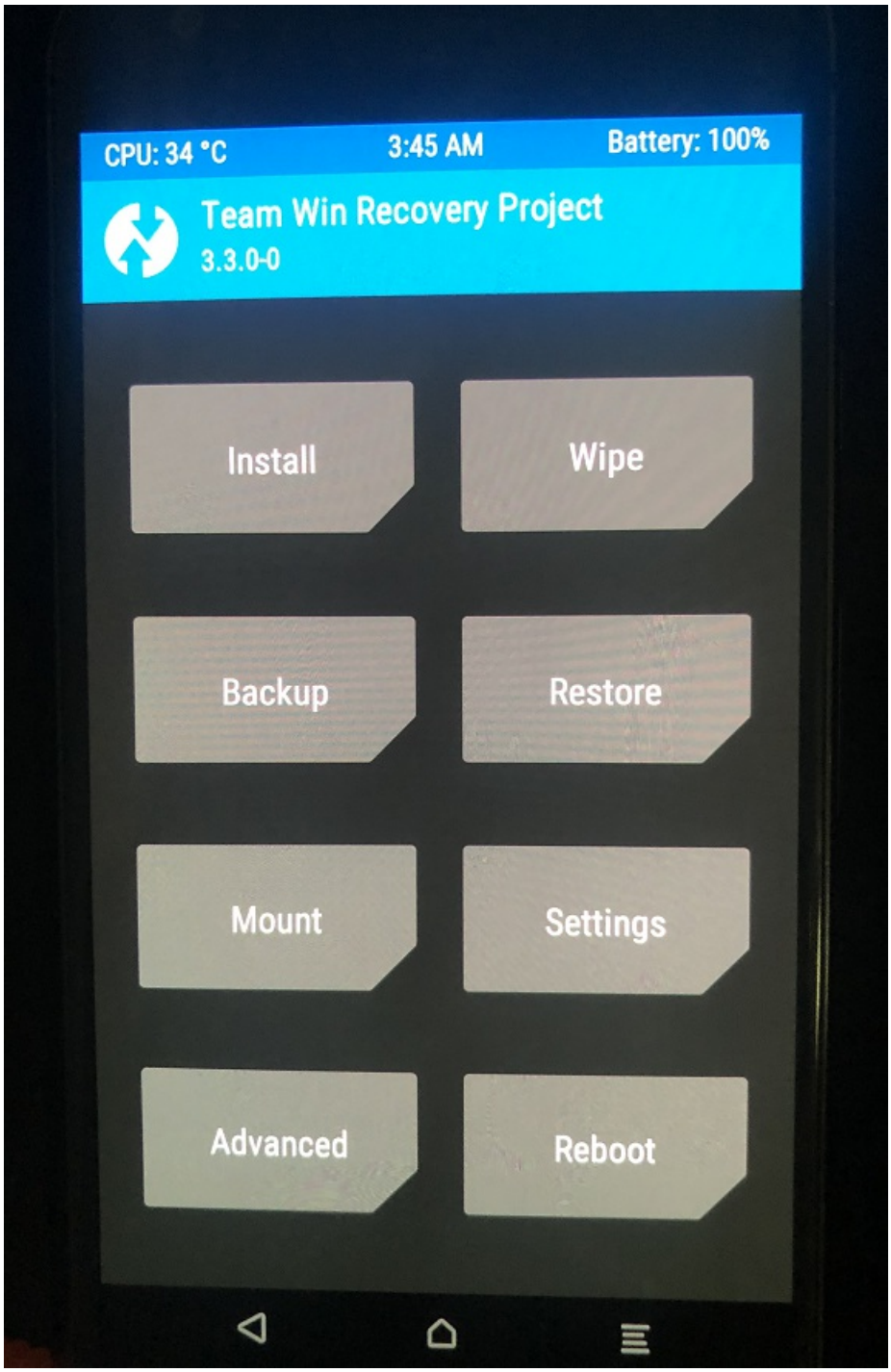
```
fastboot boot twrp-3.3.0-0-sailfish.img
```

```
root@roysue:~/Desktop# fastboot boot twrp-3.3.0-0-sailfish.img
Sending 'boot.img' (31000 KB)                      OKAY [  3.563s]
Booting                                            OKAY [  0.903s]
Finished. Total time: 4.478s
```

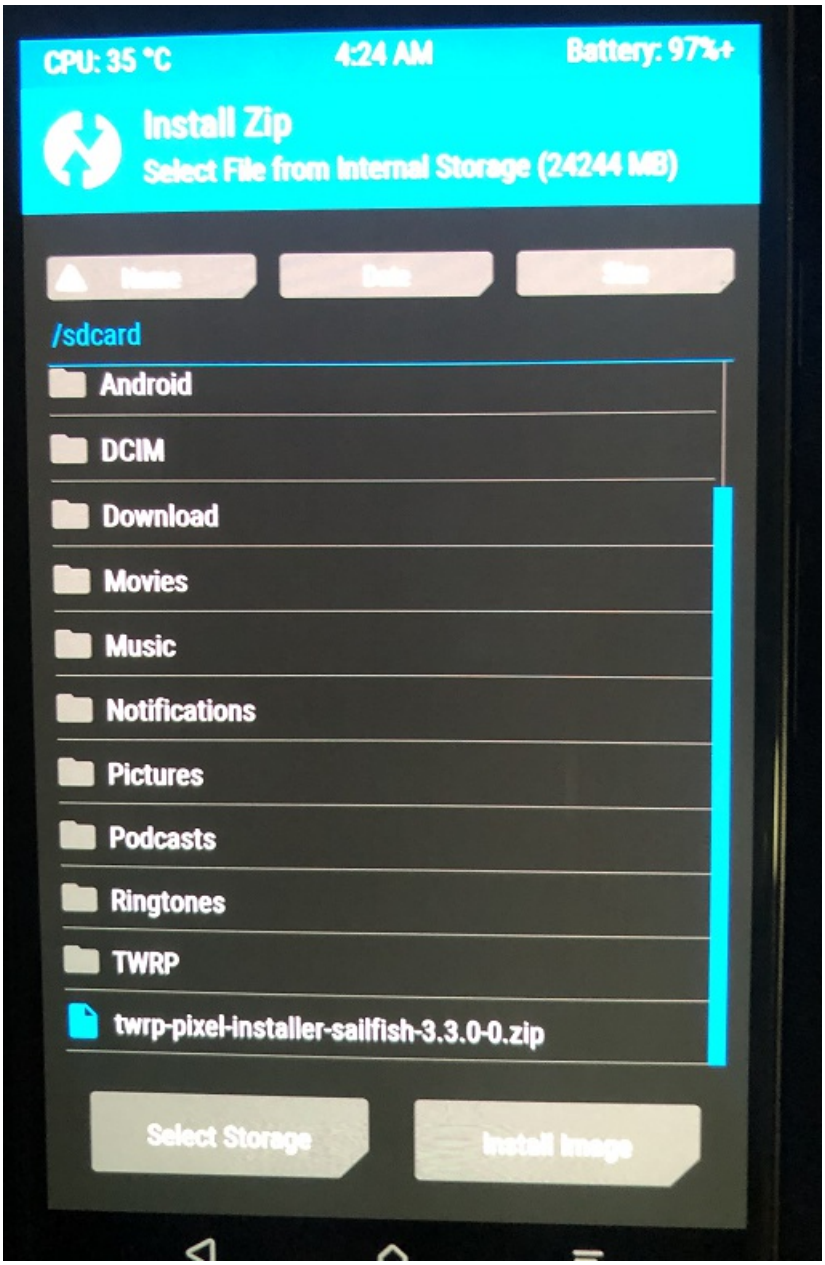
3、这个时候手机会自动重启，并进入twrp的安装界面。



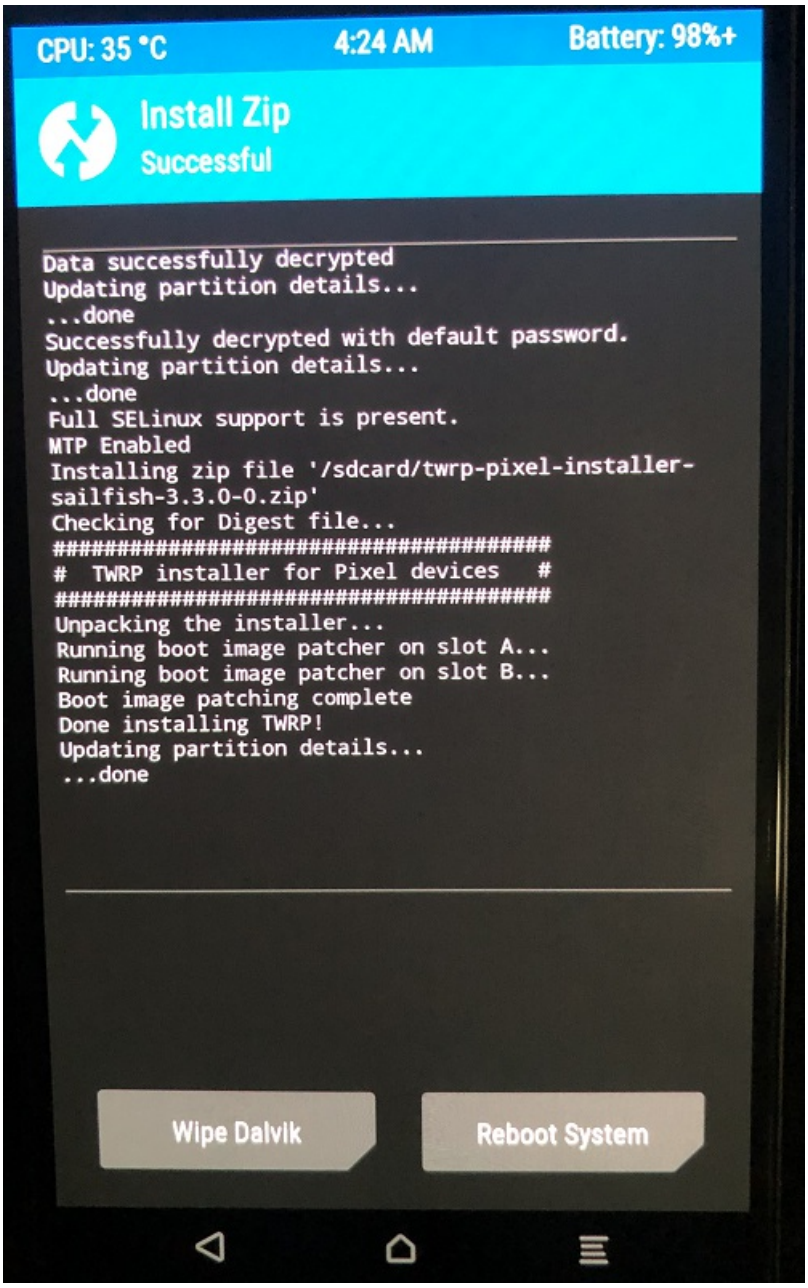
4、滑动下方的滑块，进入安装界面



5、点击install会进入到类似文件管理器的界面，在这里可以看到1中push的zip包，点击它



6、同样会有一个滑块，滑过去之后就进入到下面这个界面了。



7、点击Reboot System完成twrp的刷入

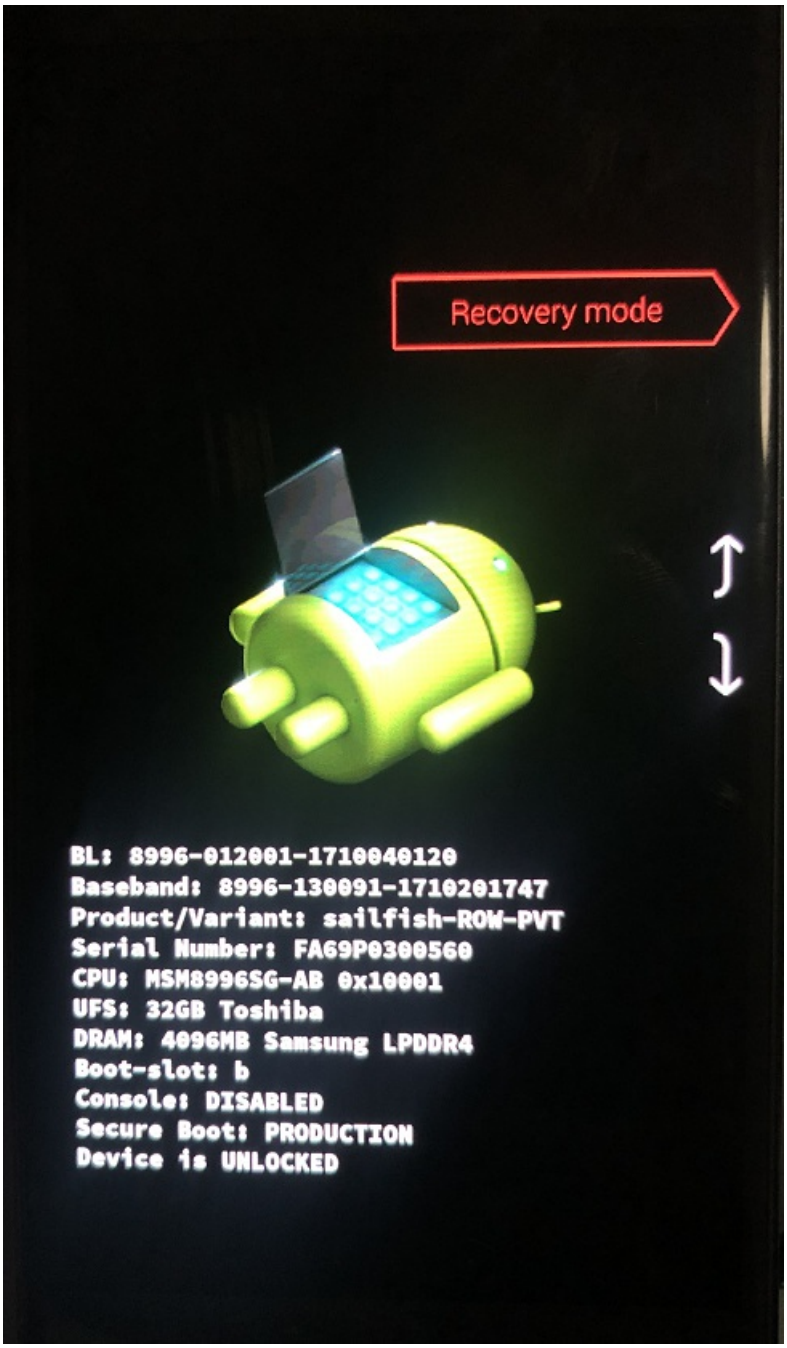
三、刷入 Magisk 完成 Root

1、准备好安装包Magisk-v20.4.zip，使用下面的命令push进去

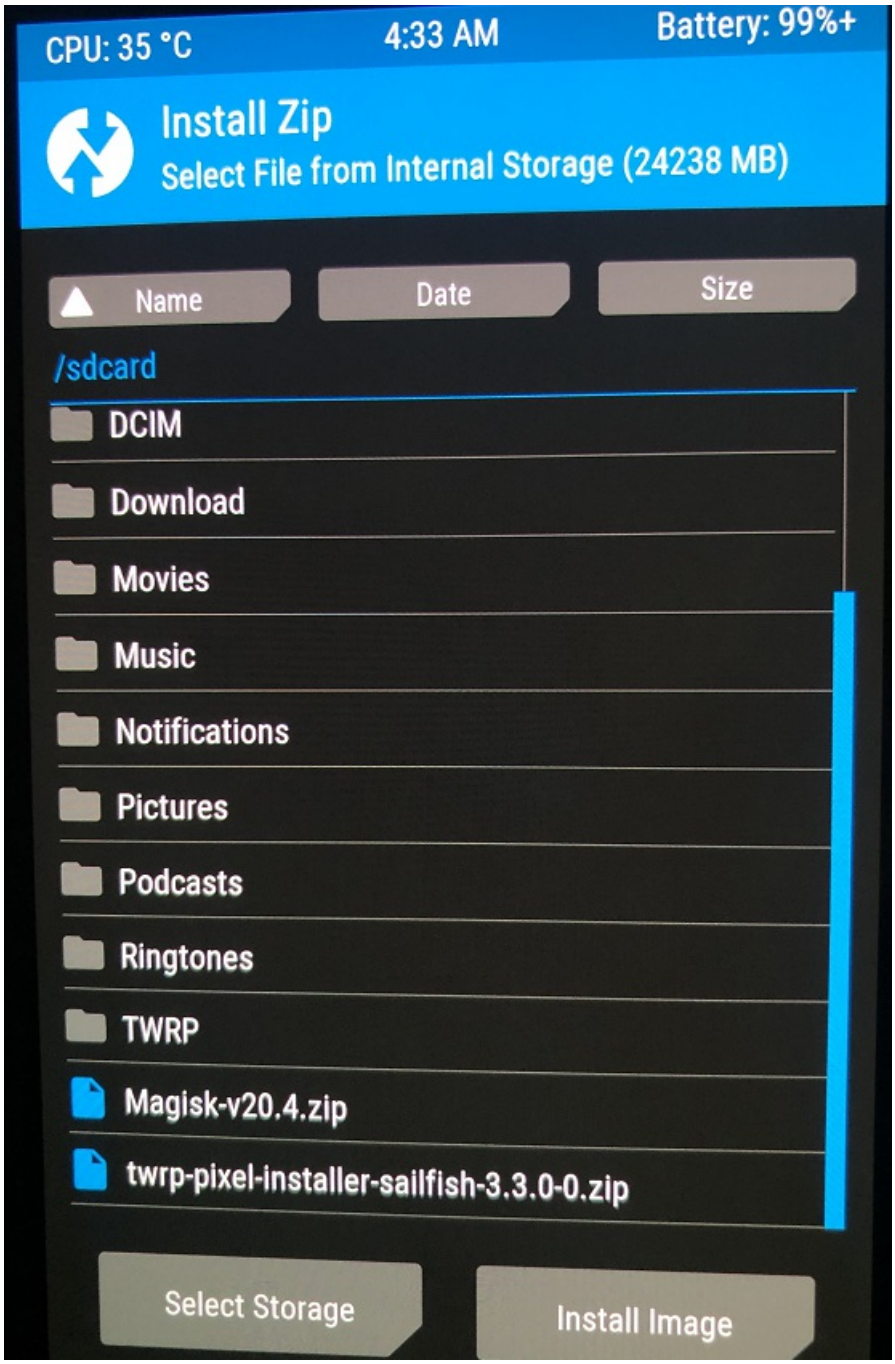
```
adb push /yourpath/Magisk-v20.4.zip /sdcard
```

```
root@roysue:~/Desktop# adb push Magisk-v20.4.zip /sdcard/
Magisk-v20.4.zip: 1 file pushed, 0 skipped. 17.3 MB/s (5942417 bytes in 0.328s)
```

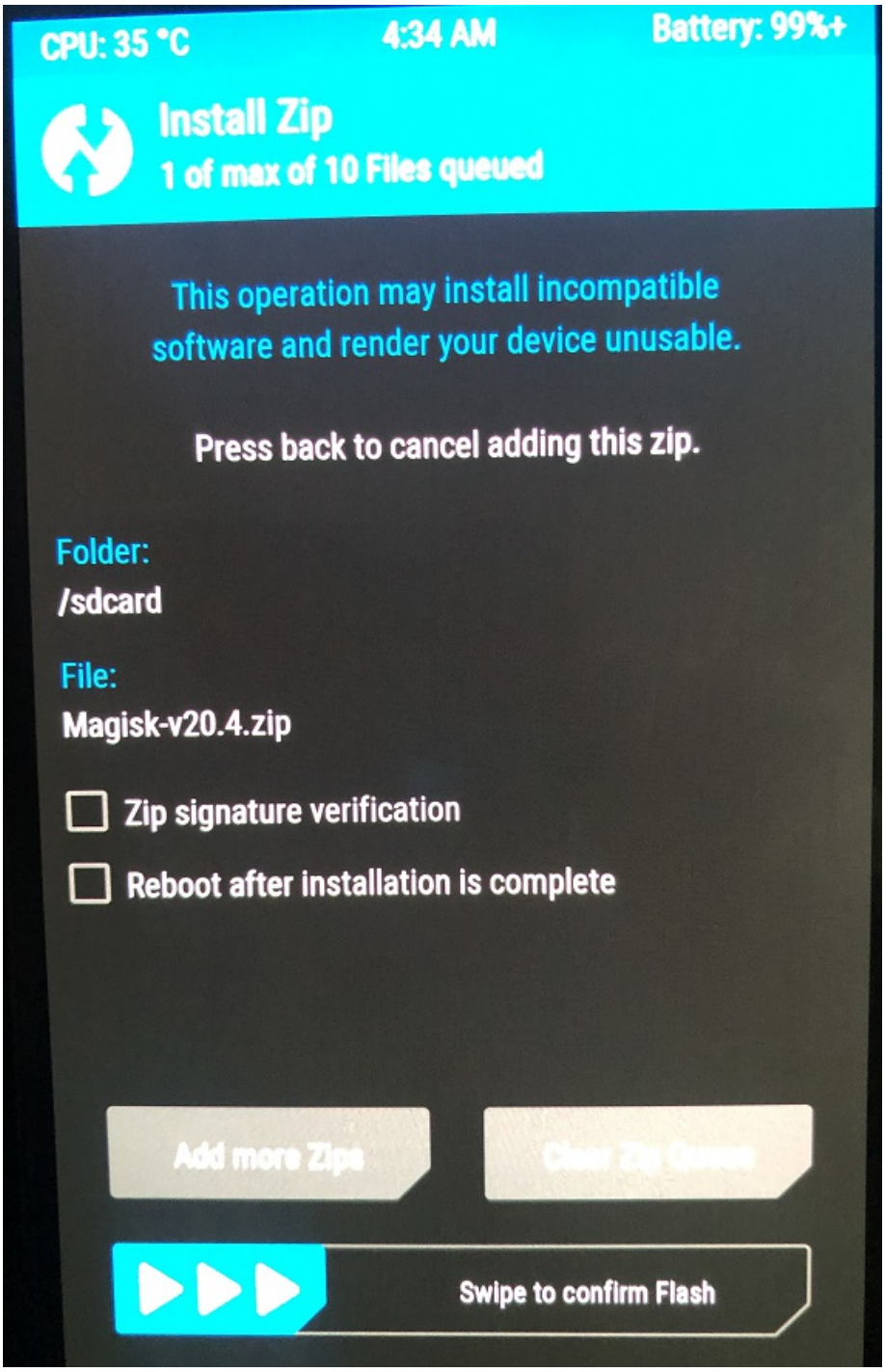
2、将手机设置为fastboot模式，并且按动音量键切换至Recovery模式，并按电源键选中，这个时候手机会启动，并进入twrp的安装界面。



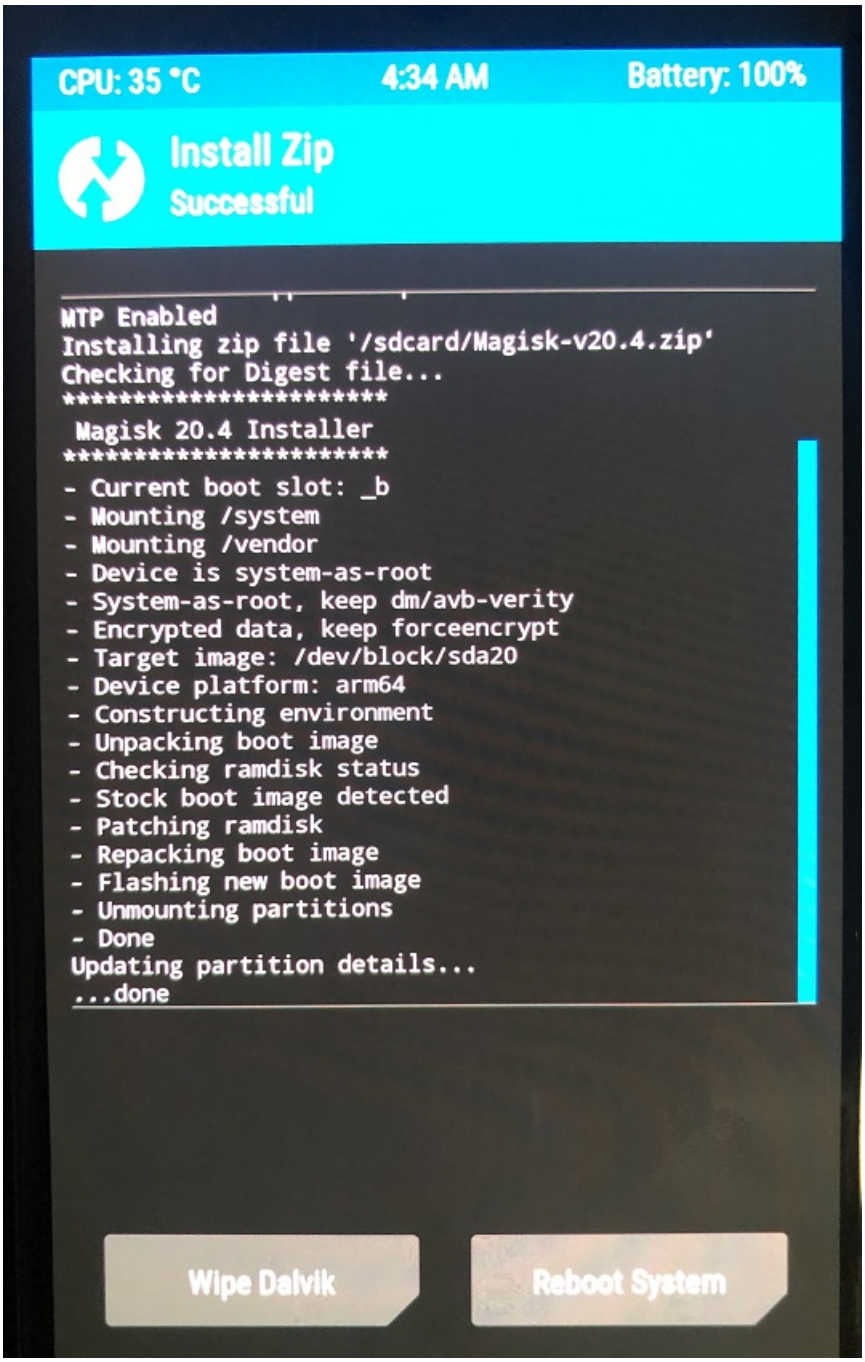
3、重复刷入twrp这节中的3、4步，在列表中选中本节第 1 步中push的zip包



4、同样还是滑块，进入安装



5、滑过去后就进入到安装界面了



6、安装完成，点击`Reboot System`完成`Magisk`的安装

7、安装完成后，使用`adb shell`连接手机，使用下面的命令获取`root`权限

```
su -
```

这个时候手机会有弹窗记得点击确定就可以了

```
sailfish:/ # whoami
root
sailfish:/ #
```

四、Frida-Server 的安装

1、获取软件包后，使用`adb push`将解压好的文件推送至手机

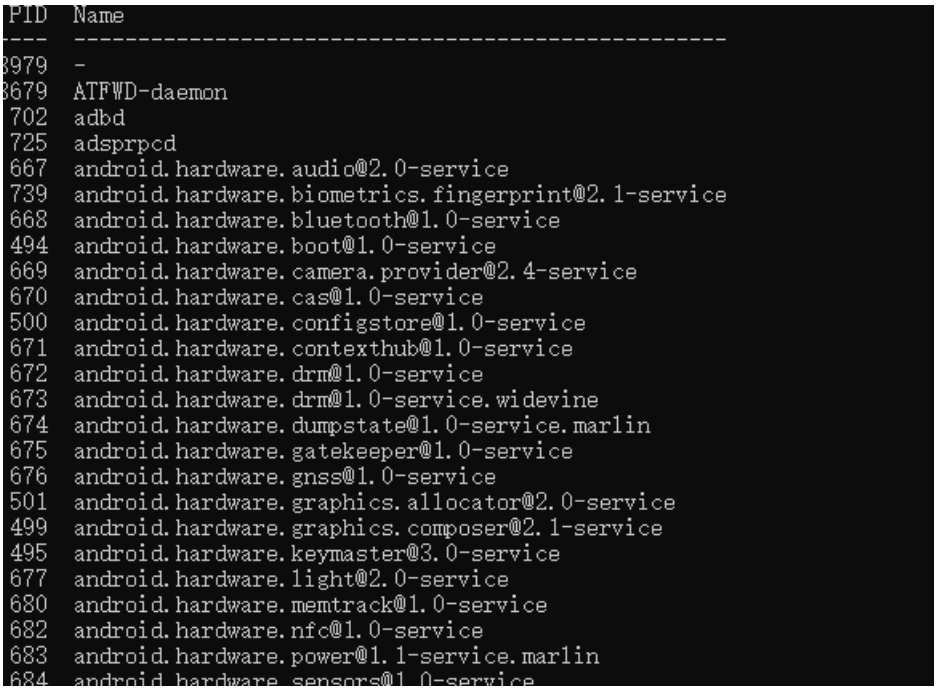
```
adb push /yourpath/frida-server-12.8.0-android-arm64 /data/local/tmp
```

2、推送后，使用`adb shell`连接手机，切换至`/data/local/tmp`下，运行即可开启

```
./frida-server-12.8.0-android-arm64
```

3、开启后重新打开一个电脑的`shell`，注意下面这行命令实在你的电脑上运行的，不是在手机上

```
frida-ps -U
```



得到上面的回显代表成功

如果出现明明启动了手机上的`server`但是电脑连不上可以杀死手机上的`server`的进程

```
ps | grep frida
kill -9 fridapid
./frida-server-12.8.0-android-arm64 &
```

五、踩坑记录

得益于肉丝姐的手把手教学整个过程安装比较顺利，我自己就遇到一个关于 VM 的坑

这里推荐一下肉丝的逆向课，进阶版的可以扫下面这个码了解详情。

（解释一下：扫码购买我是没有佣金的，别喷了）

如果你感觉上面这个太过专业，可以找肉丝 Py 下，他还有一个专为爬虫er 开设的零基础逆向班，我就不贴代码了，少一个人学会少一点竞争力 

继续说我遇到的坑：

1、虚拟机软件不要使用 VM 的 15.0 这个版本，使用更高的版本或者低一点的版本，15.0 这个版本在第一节刷机的时候会出现 VM 卡死的情况

同时可以参考其他大佬的笔记

```
https://mp.weixin.qq.com/s/8XoPinibc12SE-Ru5fXjdg
```

在上面这篇文章的结尾也提到了一个坑，是关于twrp中出现多个加密文件的问题，所幸我没遇到，有遇到的可以参考一下解决办法

下面这段解决方案来自公众号：编程这块不如你

```
刷入临时 TWRP 老是会出现 /sdcard/ 下面显示类似加密的多个文件,进 TWRP(Advanced Wipe/Format) 后重新 flash-all 也没效

解决方法：Wipe - Advanced Wipe - 选Internal Storage - Swipe to Wipe(一定要确认/sdcard/下面没有任何内容,有时候wipe
```

完成上面的步骤之后就可以继续 Frida 学习之旅了，下次再会~

[完]

咸鱼学Python

微信扫描二维码，关注我的公众号