```
AOSP源码编译和刷入和内核编译8.1.0_r1
系统: kali 19.04
手机型号: pixel
系统版本: 8.1.0_r1
初始编译命令与712r8的过程一致
# 命令行
内核编译过反调试,使ptraceid始终为0
cd ../kernel/
git clone https://aosp.tuna.tsinghua.edu.cn/android/kernel/msm.git
                                                              //下载内核源码
cd msm/
git checkout 1292056
                                                              //检测
nano fs/proc/base.c
                                                                //修改源码
proc_pid_wchan
      else {
            if (strstr(symname, "trace")) {
                   return seq_printf(m, "%s", "sys_epoll_wait");
                   return seq_printf(m, "%s", symname);
      }
nano fs/proc/array.c
static const char * const task_state_array[] = {
      };
seq_printf(m,
            "TracerPid:\t0\n"
            ppid, /*tpid,*/
编译
apt install bc
                                                              //安装所需库
apt-get install liblz4-tool
export ARCH=arm64
                                                              //设置目标架构
export PATH=$PATH:/root/Desktop/COMPILE/aosp810r1/prebuilts/gcc/linux-x86/aarch64/aarch64-linux-android-
4.9/bin //将工具集加入路径中
export CROSS_COMPILE=aarch64-linux-android-
                                                               //设置联合编译方式
make marlin-defconfig
                                                              //准备编译
make
重新编译镜像文件
source build/envsetup.sh
lunch
export TARGET_PREBUILT_KERNEL=/root/Desktop/COMPILE/aosp810r1/kernel/msm/arch/arm64/boot/Image.lz4-dtb
//选择所需内核镜像
make bootimage
                                                               //制作新的boot.image
替换后刷机
./flash-all.sh
# 需注意问题
涉及到内核的东西坑都很多
修改内核源码过程中一定要注意不要修改错误
这个内核源码改完之后可以实现过ptarcepid反调试位的方法
# 待解决问题
R姐把文章和官方文档都已经读烂掉了
找个时间好好读几遍
                           × 1 4:41
?
     About phone
\leftarrow
     Legal information
     Regulatory labels
```

Model

AOSP on msm8996

Android version

8.1.0

Android security patch level

December 5, 2017

Baseband version

8996-130091-1710201747

Kernel version

3.18.70-g5fa7e7d4ea9e-dirty (gcc version 4.9.x 20150123 (prerelease) (GCC)) root@darenfy #1 Wed Apr 29 22:34:30 EDT 2020

Build number

aosp_sailfish-userdebug 8.1.0 OPM1.171019.011 eng.root.20200428.215105 test-keys

 \triangleleft



