# TODO

https://blog.csdn.net/viewsky11/article/details/54906599

# external/conscrypt

# Tcpdump

可以用网上下载的

adb shell tcpdump -n -vvv -c 1000 -w /sdcard/tcpdump\_ok.cap

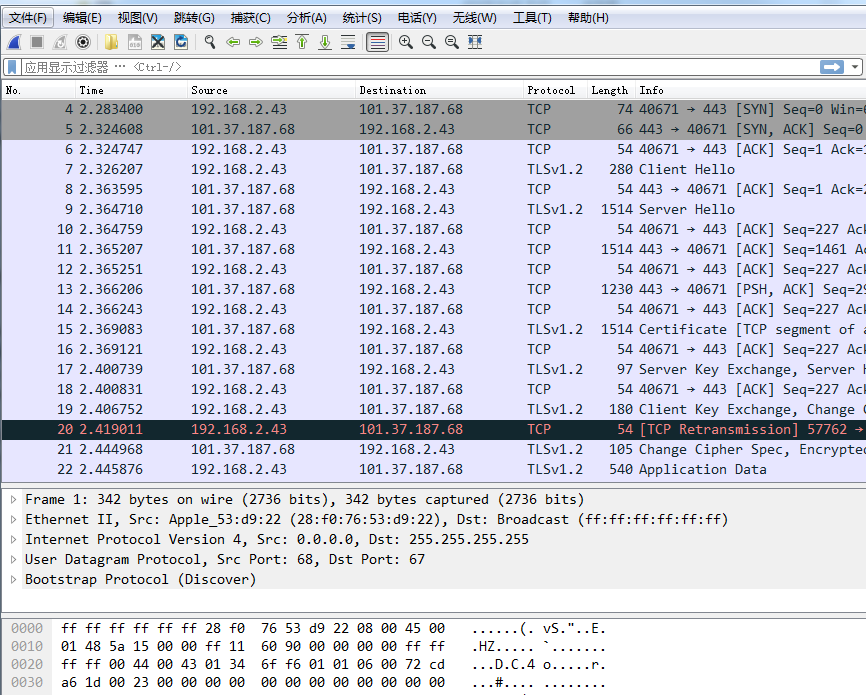
root后

把tcpdump放到/system/xbin下 chmod +x tcpdump

绑定ip

adb shell cat /system/etc/hosts

ping www.skypixel.com



tonicsystems

iptable

android-7.1.1\_r1/external/iptables/iptables/iptables.c

# wpa\_supplicant

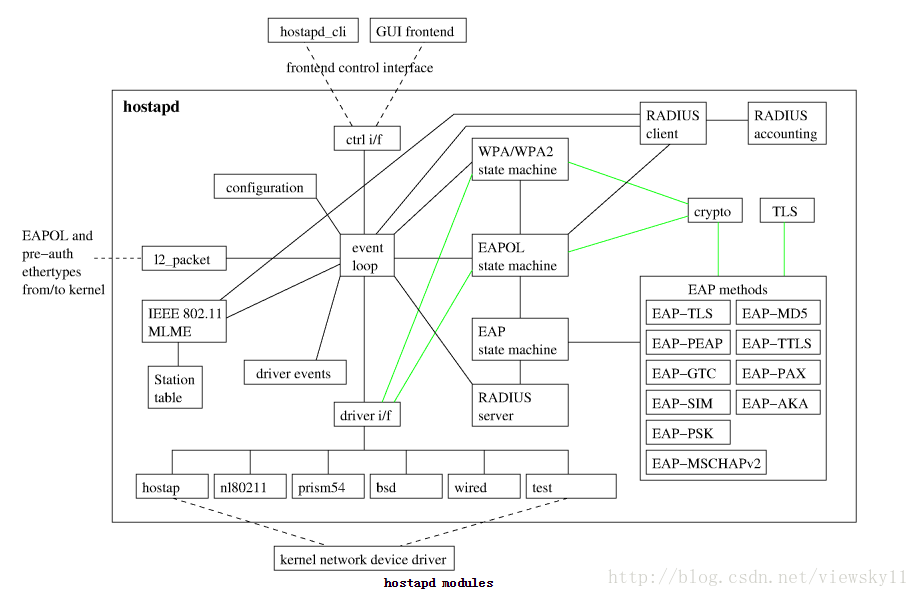
 生成库libwpaclient.so和守护进程wpa\_supplicant

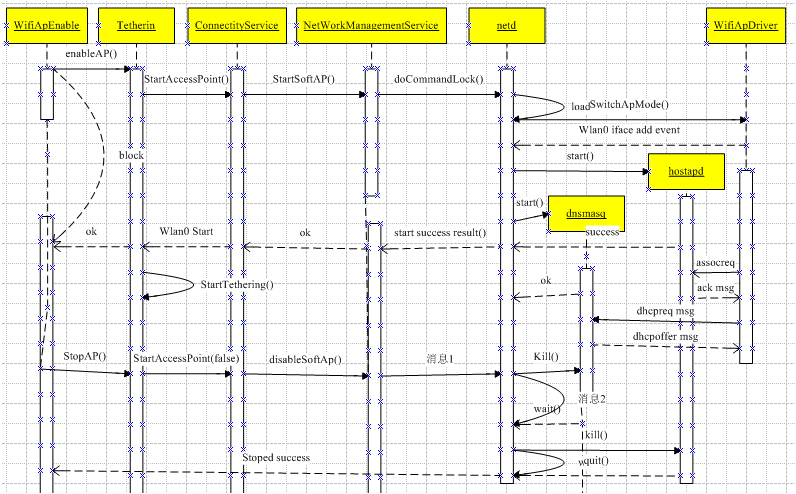
# Hostapd

external/wpa\_supplicant\_8/hostapd/Android.mk

Hostapd的功能就是作为AP的认证服务器，负责控制管理stations(通常可以认为带无线网卡的PC)的接入和认证。

通过Hostapd可以将无线网卡切换为AP/Master模式，通过修改配置文件，可以建立一个开放式的(不加密)的，WEP，WPA或WPA2的无线网络。并且通过修改配置文件可以设置无线网卡的各种参数，包括频率，信号，beacon包时间间隔，是否发送beacon包，如果响应探针请求等等。还可以设置mac地址过滤条件等





# 实战

## 监听设备接入

01-18 17:05:40.066 567-567/? I/wificond: New station ec:d0:9f:b0:df:97 associated with hotspot

01-18 17:05:39.048 582-582/? I/chatty: uid=1000(system) /system/bin/ATFWD-daemon identical 1 line

01-18 17:05:40.049 582-582/? I/ServiceManager: Waiting for service AtCmdFwd...

01-18 17:05:40.066 4530-4530/? I/hostapd: wlan0: STA ec:d0:9f:b0:df:97 IEEE 802.11: associated

wlan0: STA ec:d0:9f:b0:df:97 IEEE 802.11: associated

wlan0: AP-STA-CONNECTED ec:d0:9f:b0:df:97

通过日志来看，我们至少可以从wificond或者hostapd来寻找分析，由于开放的是热点，

因此我们直接分析hostapd。

android7没有wificond

android8才有wificond

## android7

wificond