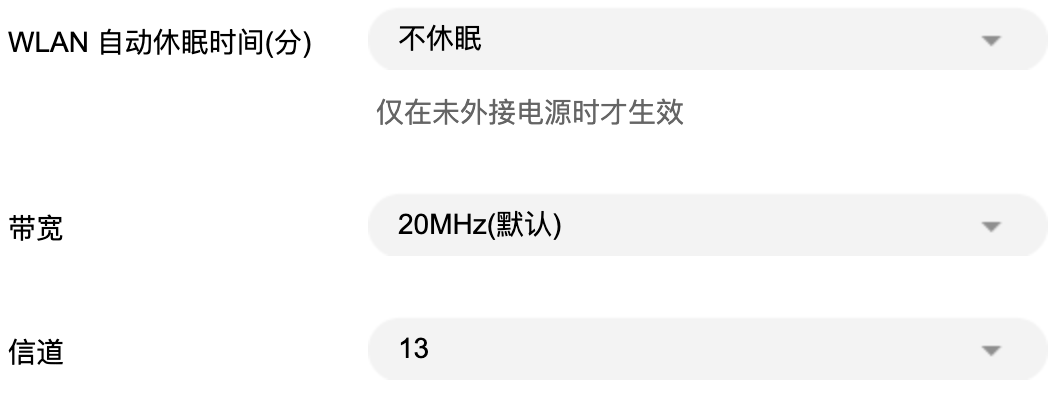
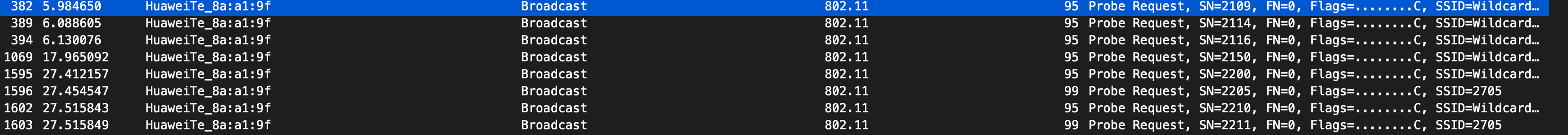
AP设置

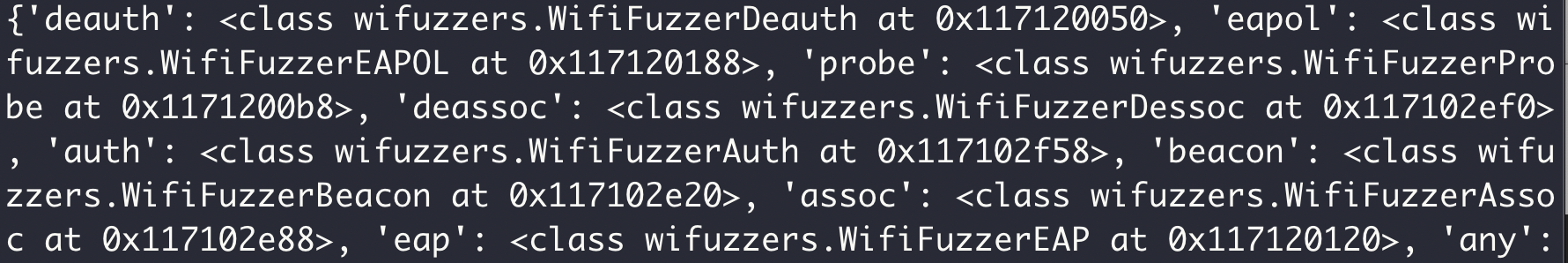
网络设置，配置AP加密方式：

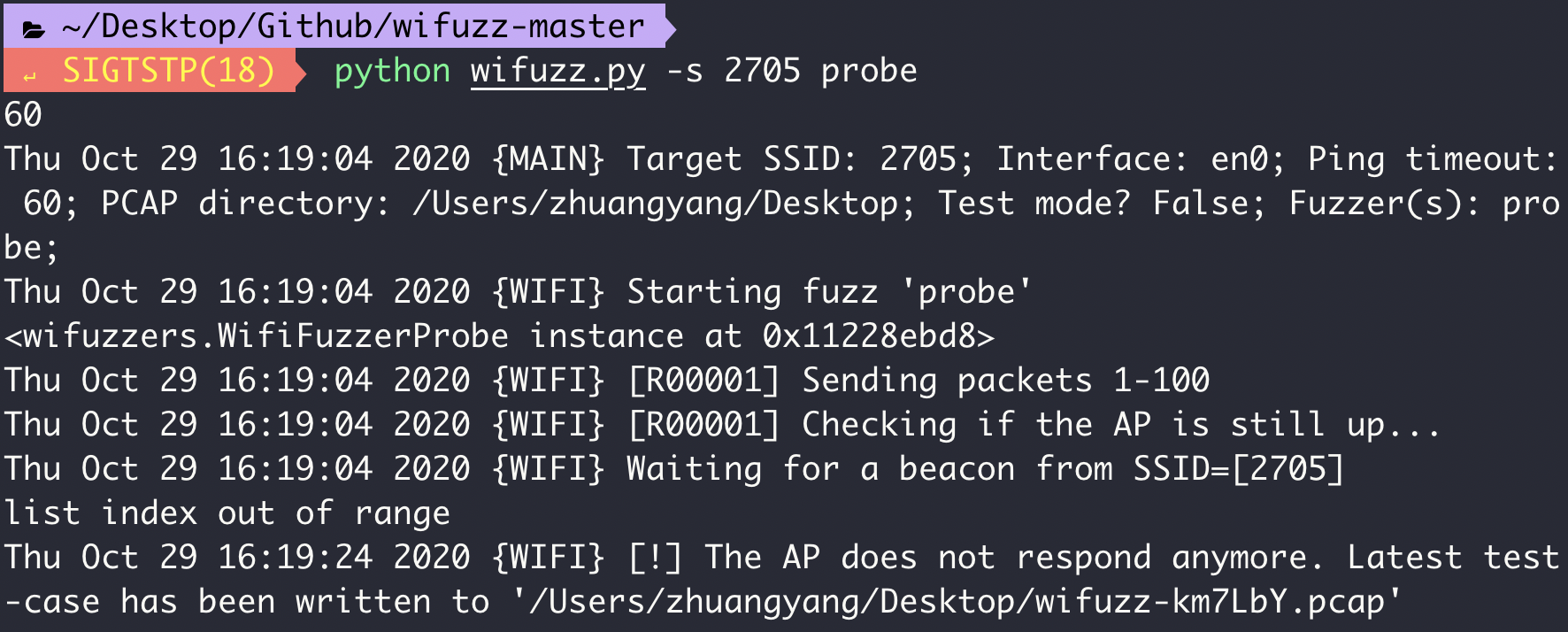
配置信道：

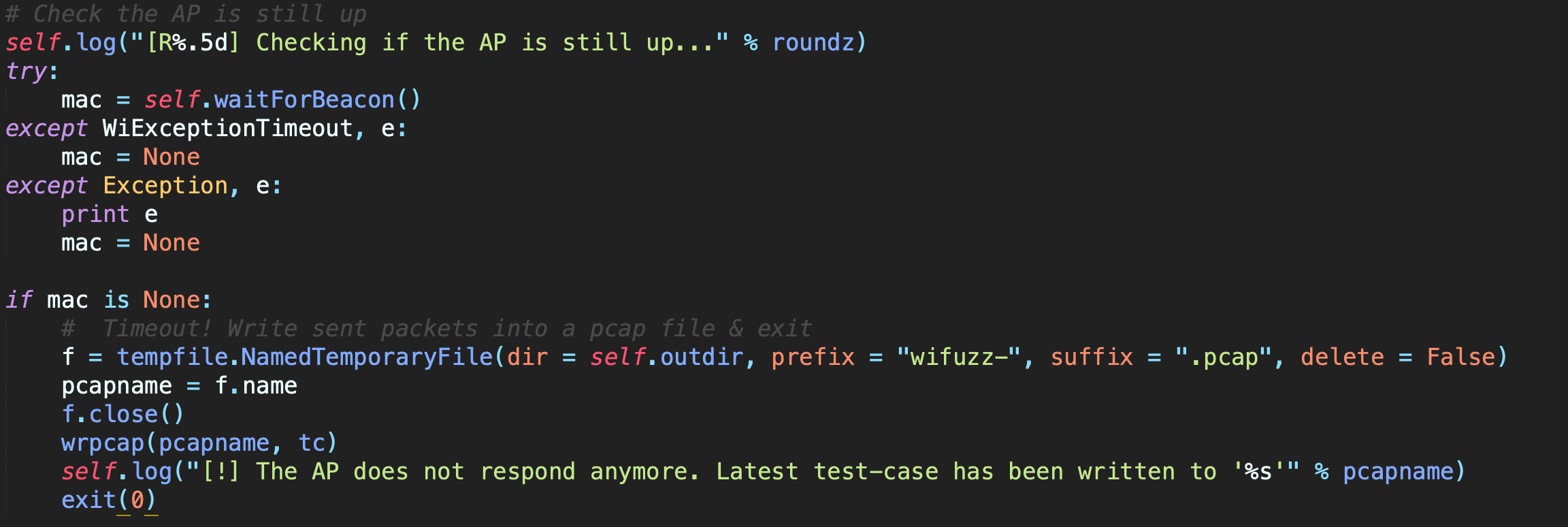
问题1:Beacon脚本运行后在手机上无法获取到SSID

不同设备实现对于probe request的时间点和方式不一样：

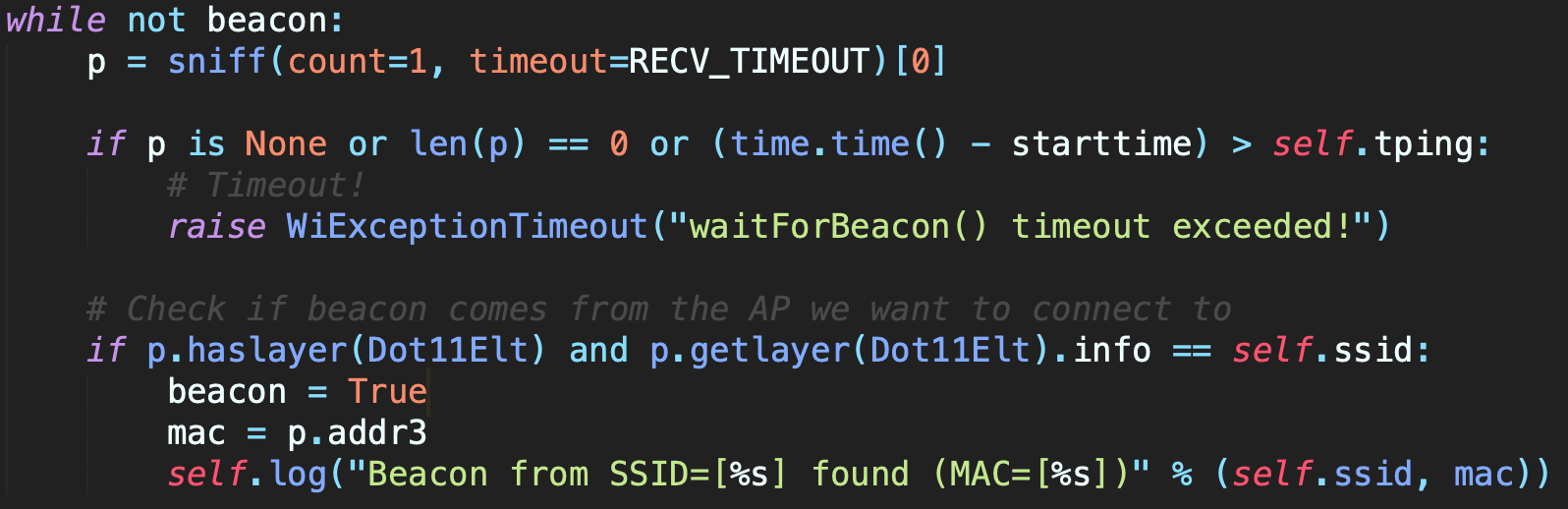
Wifuzz测试

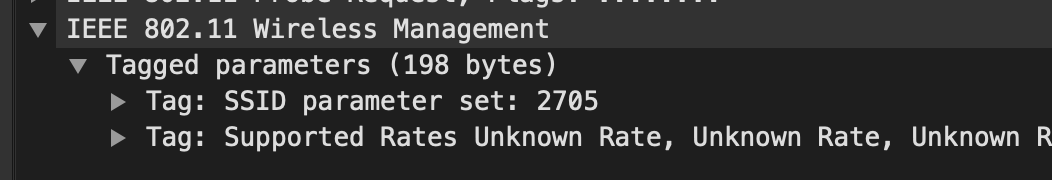
实际支持的帧类型：

probe Request帧

Probe Request的fuzz相对简单，发出的帧理论上AP都会解析。wifzz采用的check alive机制是监听AP是否依然不断发送beacon帧：

另外，看代码觉得这个实现很奇怪，并没有很好的检测是否是Beacon帧：



Wifuzz构造的Probe Request相对比较简单，并没有对只对两个EI进行fuzz：

Wifuzzit

CFuzz

实验1:确认发送Beacon帧STA能扫描到对应的SSID（Scapy）

实验2:捕获Probe Request帧之后能够回复Probe Response帧（Scapy）

实验3:通过侦听probe Request请求后构造Probe Response，同时监听ACK包确认发送数据包成功

实验4:通过监听Authentication帧和Association Request回复Authentication帧和Association Response，同时监听ACK帧，结果是手机能连上fake AP但是提示没有IP地址。

实验5:验证Probe response是否被解析，因为并不是所有返回ACK的帧都被解析。通过发送递增次序的SSID观察是否有丢包来判断。