

Misc: ngc's wifi

题目给了一个数据包，打开来看都是 802.11 协议

所以是破解 WIFI 密码题目

放到 kali 里分析

```
root@kali: ~/Desktop/1
牛(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@kali:~/Desktop/1# aircrack-ng flag2.cap
Loading flag2.cap
Loaded 109554 packets.

# BSSID Music ESSID Encryption
1 88:25:93:1E:99:D2 TP-LINK_99D2 WPA (0 handshake)
2 64:CC:2E:75:7D:27 ngc's wifi2 WPA (1 handshake)
3 A8:6B:7C:2F:BB:1B 360WiFi-111 WPA (0 handshake)
4 54:36:9B:00:46:85 lixin WPA (1 handshake)
5 7C:B5:40:0F:BB:B0 ChinaMobile_5055 WPA (0 handshake)
6 6F:B2:D6:E6:A4:DB Unknown
7 B4:49:16:72:B7:97 Unknown
8 A5:23:F9:82:56:56 Unknown
9 EC:26:CA:71:36:C4 TP-LINK_36C4 WPA (0 handshake)
0 67:19:57:04:2F:52 Unknown
1 EE:4A:1F:D8:61:02 WEP (1 IVs)
2 64:48:2F:43:73:E0 Unknown
3 80:F0:CE:62:E4:EE Unknown
```

在 kali 里分析一波之后，hint 给出了密码是手机号码 并且是 ngc（潍坊）的手机号码

于是我先找到了 ngc 学长的 QQ 号，通过腾讯的找回密码缩小范围

请输入您绑定的密保手机号：

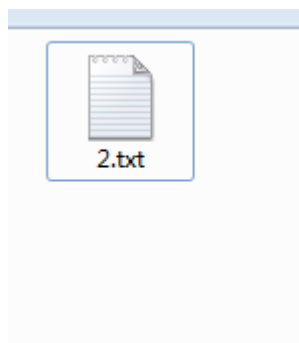
133\*\*\*\*\*

完整的手机号

确定

记不清了？[更换其他验证方式](#)

既然是 133 开头，潍坊的，网上搜集到潍坊以 133 开头的手机号码，打包成 txt 文件形式



字典有了 就跑吧

```
root@kali: ~/Desktop/1
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

Aircrack-ng 1.2 rc4

[00:02:01] 494460/576212 keys tested (3747.51 k/s)

Time left: 21 seconds 85.81%

KEY FOUND! [ 13375369512 ]

Master Key      : 9B 5C 3B 5B 3F 25 69 62 69 B5 BA 68 33 46 ED 67
                  FA F0 0D 16 9A B4 76 E4 A2 BB 11 B8 ED 68 77 E2

Transient Key   : 70 91 68 49 97 2C 1B 3D A9 FE 1C CF CC 6C 35 E8
                  FB 81 40 A0 10 5D 17 E7 D8 FC AF 21 B7 43 76 78
                  2C 3A D5 CB B4 27 81 C0 C8 61 D3 18 40 A7 D4 96
                  D5 85 76 05 F0 32 31 51 DD 3B 9D A6 2E 96 35 06

EAPOL HMAC     : B1 83 7E F7 06 7B 37 98 34 B6 3B 45 FC F2 D8 9D
root@kali:~/Desktop/1#
```