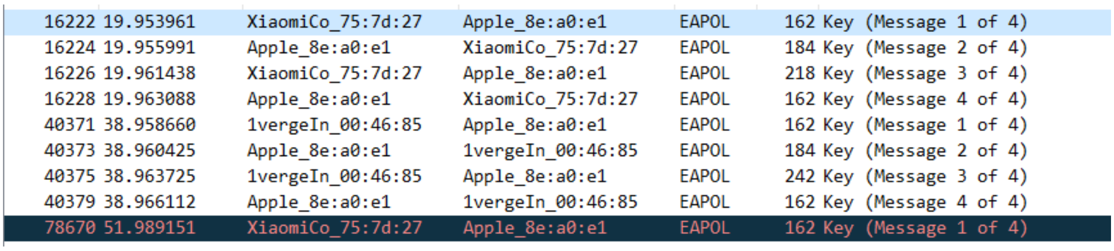
Hgame2018week4

Misc 部分

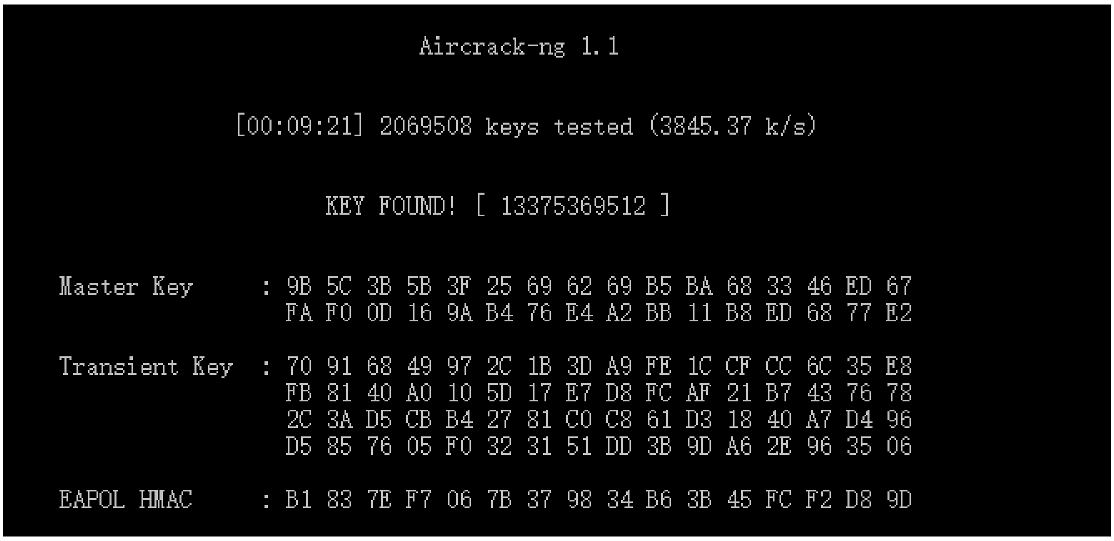
0x01 ngc's wifi

打开发现基本都是 802.11 协议的包，过滤一下 eapol 协议发现 8 次握手包，题目说是破解 ngc 的 wifi 那么应该是前 4 次



```
16222 19.953961   XiaomiCo_75:7d:27   Apple_8e:a0:e1      EAPOL   162 Key (Message 1 of 4)
16224 19.955991   Apple_8e:a0:e1      XiaomiCo_75:7d:27   EAPOL   184 Key (Message 2 of 4)
16226 19.961438   XiaomiCo_75:7d:27   Apple_8e:a0:e1      EAPOL   218 Key (Message 3 of 4)
16228 19.963088   Apple_8e:a0:e1      XiaomiCo_75:7d:27   EAPOL   162 Key (Message 4 of 4)
40371 38.958660   1vergeIn_00:46:85   Apple_8e:a0:e1      EAPOL   162 Key (Message 1 of 4)
40373 38.960425   Apple_8e:a0:e1      1vergeIn_00:46:85   EAPOL   184 Key (Message 2 of 4)
40375 38.963725   1vergeIn_00:46:85   Apple_8e:a0:e1      EAPOL   242 Key (Message 3 of 4)
40379 38.966112   Apple_8e:a0:e1      1vergeIn_00:46:85   EAPOL   162 Key (Message 4 of 4)
78670 51.989151   XiaomiCo_75:7d:27   Apple_8e:a0:e1      EAPOL   162 Key (Message 1 of 4)
```

提示说密码是手机号，还提示是潍坊，网上找了个全国手机号字典生成器生成了山东潍坊的手机号字典，拿到 air-crackng 里跑一下得到密码 13375369512



```
                              Aircrack-ng 1.1


                 [00:09:21] 2069508 keys tested (3845.37 k/s)


                        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
```

加上格式得到 flag:hgame{13375369512}