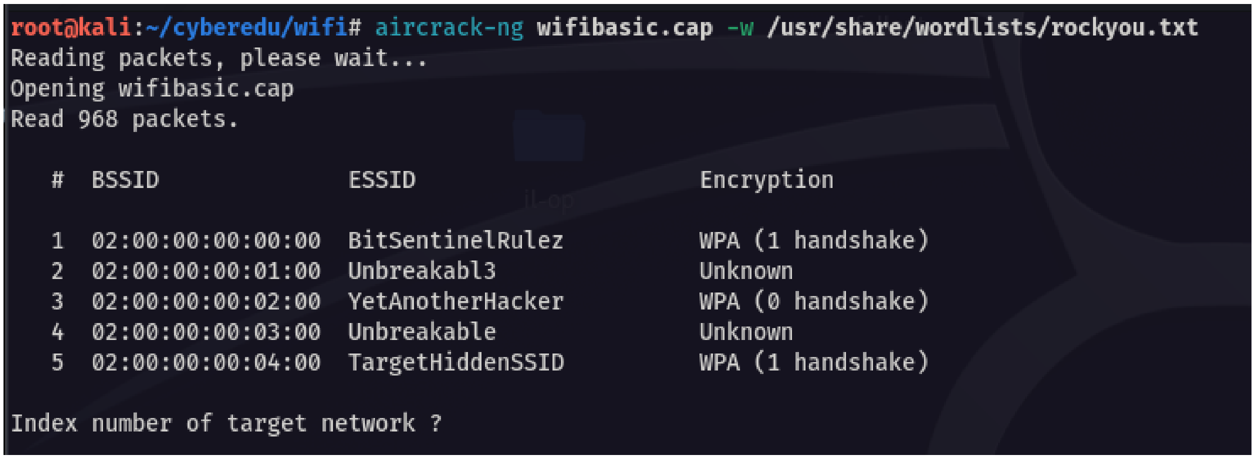
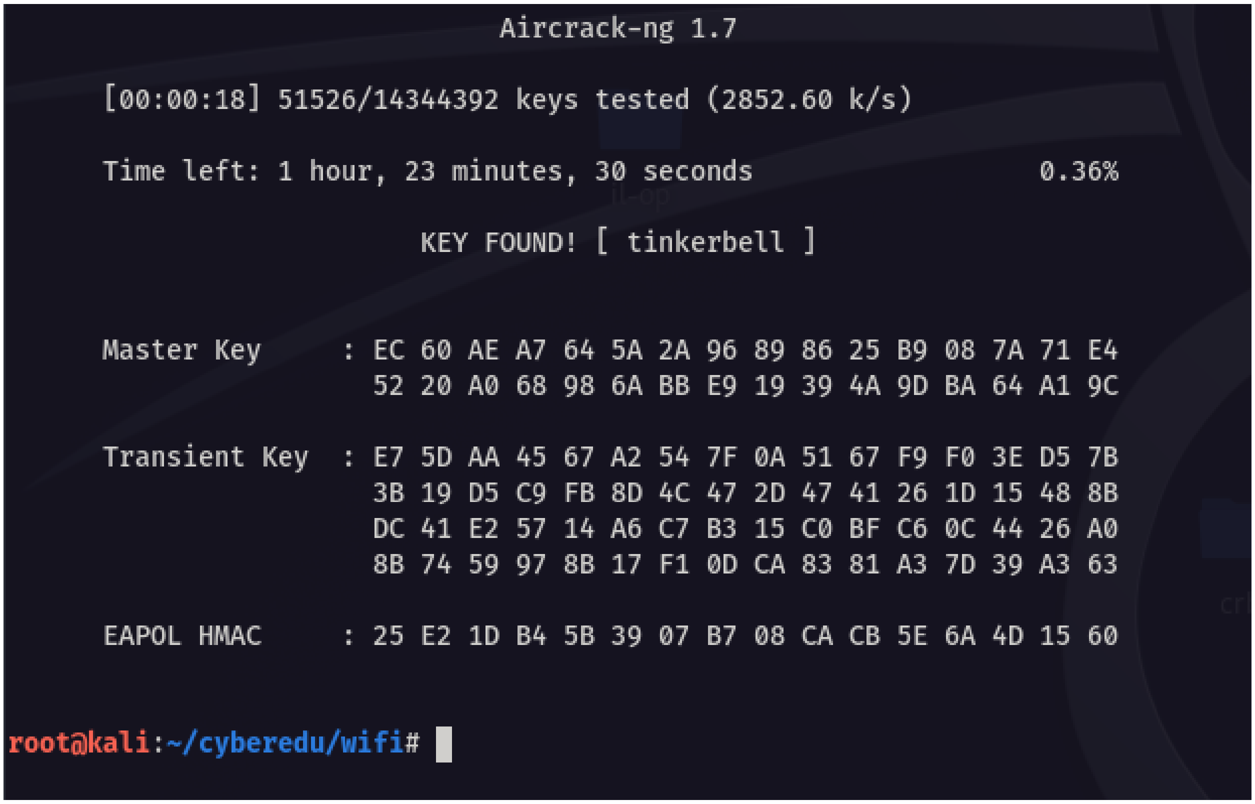
We got a wifi traffic capture file it contains a wpa handshake.



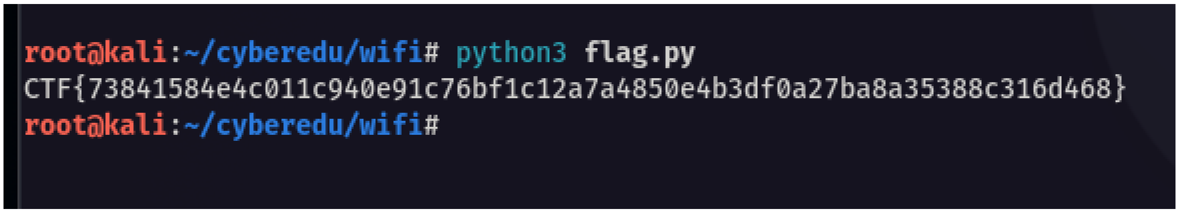
```
root@kali:~/cyberedu/wifi# aircrack-ng wifibasic.cap -w /usr/share/wordlists/rockyou.txt
Reading packets, please wait...
Opening wifibasic.cap
Read 968 packets.

   #  BSSID              ESSID                     Encryption

   1  02:00:00:00:00:00  BitSentinelRulez          WPA (1 handshake)
   2  02:00:00:00:01:00  Unbreakabl3               Unknown
   3  02:00:00:00:02:00  YetAnotherHacker          WPA (0 handshake)
   4  02:00:00:00:03:00  Unbreakable               Unknown
   5  02:00:00:00:04:00  TargetHiddenSSID          WPA (1 handshake)

Index number of target network ?
```

We found the password



```
                               Aircrack-ng 1.7

      [00:00:18] 51526/14344392 keys tested (2852.60 k/s)

      Time left: 1 hour, 23 minutes, 30 seconds                  0.36%

                           KEY FOUND! [ tinkerbell ]


      Master Key     : EC 60 AE A7 64 5A 2A 96 89 86 25 B9 08 7A 71 E4
                       52 20 A0 68 98 6A BB E9 19 39 4A 9D BA 64 A1 9C

      Transient Key  : E7 5D AA 45 67 A2 54 7F 0A 51 67 F9 F0 3E D5 7B
                       3B 19 D5 C9 FB 8D 4C 47 2D 47 41 26 1D 15 48 8B
                       DC 41 E2 57 14 A6 C7 B3 15 C0 BF C6 0C 44 26 A0
                       8B 74 59 97 8B 17 F1 0D CA 83 81 A3 7D 39 A3 63

      EAPOL HMAC     : 25 E2 1D B4 5B 39 07 B7 08 CA CB 5E 6A 4D 15 60


root@kali:~/cyberedu/wifi# 
```

Run the python script.



```
root@kali:~/cyberedu/wifi# python3 flag.py
CTF{73841584e4c011c940e91c76bf1c12a7a4850e4b3df0a27ba8a35388c316d468}
root@kali:~/cyberedu/wifi#
```