1.1

M = {a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z}

1. H(M) = -

= -26(0.03846 \* -4.7004974271) ≈ 4.7

2.

H(M) ≈ -(-0.295 -0.091 -0.144 -0.194 -0.378 -0.122 -0.114 -0.246 -0.268 -0.014 -0.054 -0.187 -0.129 -0.262 -0.28 -0.11 -0.01 -0.243 -0.252 -0.314 -0.143 -0.065 -0.128 -0.014 -0.112 -0.008) ≈ 4.177

3.

Huffman code:

a: 1110

b: 110000

c: 01001

d: 11111

e: 100

f: 00101

g: 110011

h: 0110

i: 1011

j: 001001011

k: 0010011

l: 11110

m: 00111

n: 1010

o: 1101

p: 110001

q: 001001001

r: 0101

s: 0111

t: 000

u: 01000

v: 001000

w: 00110

x: 001001010

y: 110010

z: 001001000

長度期望值: 4.205

1.2

1. False, 因為不論key是多少，丟進去產生的結果都相同。

2. False, 當知道第i個bit，即可推測出第i+n個bit。

3. False, 攻擊者永遠都可以知道最後一個bit是0，根據定義，只要知道第i個，就可以推測出第i+1個。

4. True, 對產生出來的結果做⊕1，只是單純把0和1交換，因此無法從任何一個bit推測出其他bit。

5. True, 對key做⊕1，只是單純的把key的0和1交換，因此無法從任何一個bit推測出其他bit。

6. True, 兩個G使用的是不同的key，因此無法從任何一個bit推測出其他bit。

1.3

1. I(X;Y) =

=

= )

=

=

=

= -H(X|Y) + H(X)

= H(X) – H(X|Y)

2. 由1知，I(X;Y) = H(X) – H(X|Y)

所以 I(X;X) = H(X) – H(X|X) = H(X) – H(1) = H(X)

1.4

是，因為M=K=C，他們的space相同，所以任兩個Message被key加密後產生的機率分布一樣。

m + k (mod 256) = c

⇒ k = c - m (mod 256)

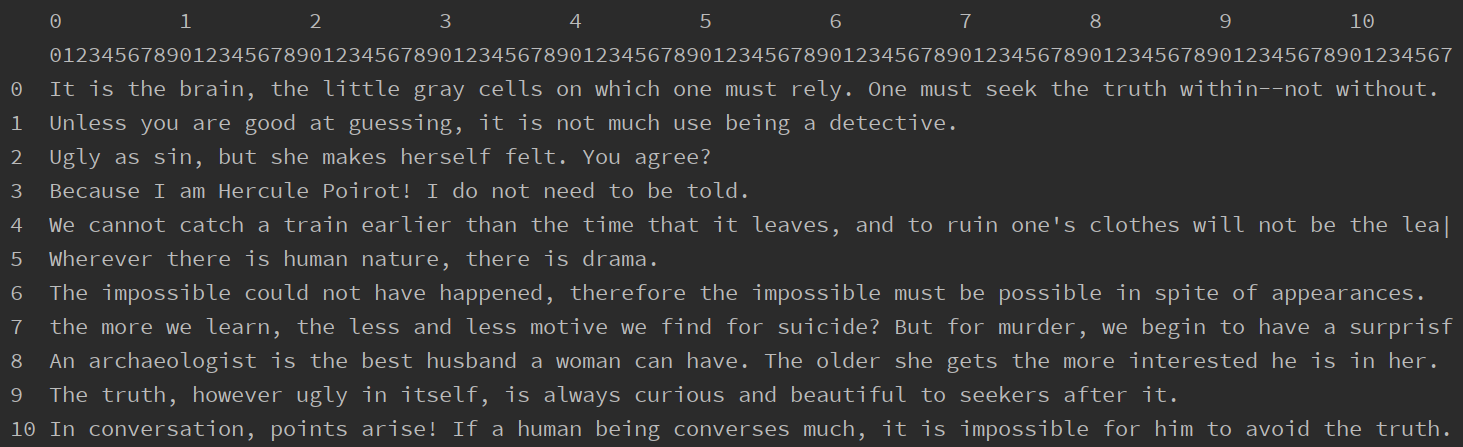
⇒ #{k ∈ K, Ek(m) = c} = 1

1.5

假設: key = 101, m0 = 000, m1 = 111

所以 c0 = 101, c1 = 010，攻擊者可以判斷出c0和m0一樣有偶數個1、c1和m1一樣有奇數個1，藉此即可分辨哪個密文對應哪個明文。

1.6

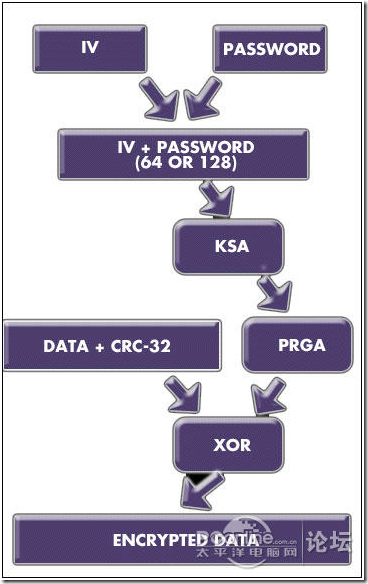


Target:

In conversation, points arise! If a human being converses much, it is impossible for him to avoid the truth.

1.7

Wep 加密原理:

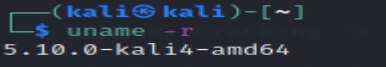


破解說明

由於WEP 在傳輸資料時，生成金鑰的初始向量IV是明文，且只有24bit，再加上封包加密的第一個位元是RC4演算法和LLC頭的第一個位元做XOR的結果，透過猜測的第一個明文與密文XOR，可得到PRNG生成金鑰的第一位，加上明文是有統計規律的語言，再搭配字典攻擊，就有極高的機率分辨兩段密文，並且可以搭配CRC校驗值，來判斷得到的猜測值是否正確。

因此WEP的破解主要透過收集大量封包(每個wep封包的標頭訊息相同)，並透過XOR運算取得部分的密碼，再收集到足夠的IV值以及部分密碼後，即可進行字典統計分析破解密碼。

系統: kali linux



無線網卡: TL-WN722N V2/V3 [Realtek RTL8188EUS]

環境處理:

光是裝網卡驅動就差點崩潰，其他東西根本秒搞定qq，剩下就只是等封包數量而已。

使用virtulbox建立虛擬環境，並在usb裝置篩選器新增無線網卡，接著安裝網卡驅動(不安裝根本不能切換到monitor mode! 搞超久!!!)，使用 apt-get install linux-headers-$(uname -r) 安裝對應kernel版本的linux-header。

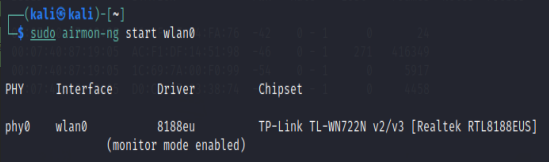
由於官網的驅動只更新到2019年，所以在官網上找不到可以對應kernel5.10版本的驅動，最後在以下網址找到對應的網卡驅動

<https://gitlab.com/kalilinux/packages/realtek-rtl8188eus-dkms>

最後按照官網驅動安裝手冊 kali 2018 年版第 10 頁指令，依序輸入，再重開機，驅動終於安裝完成，可以開始做作業了QQ。

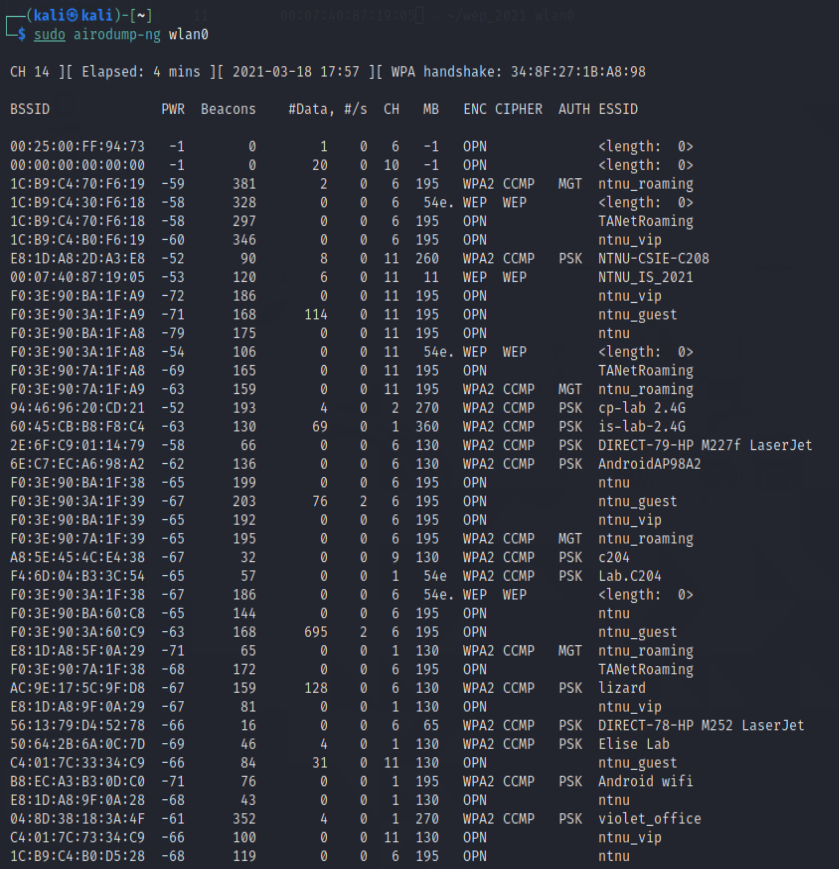
參考影片連結:

<https://www.youtube.com/watch?v=o0NKnBLHiG8&t=366s&ab_channel=CyberSpace>



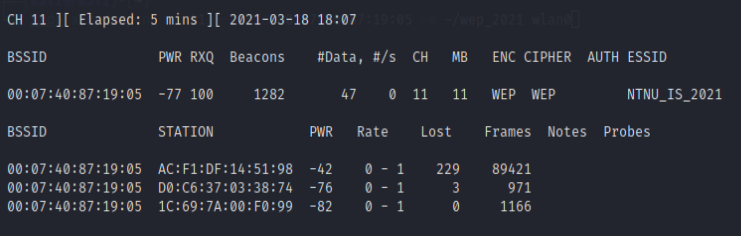
將網卡改成monitor mode，以便對wifi進行封包監控

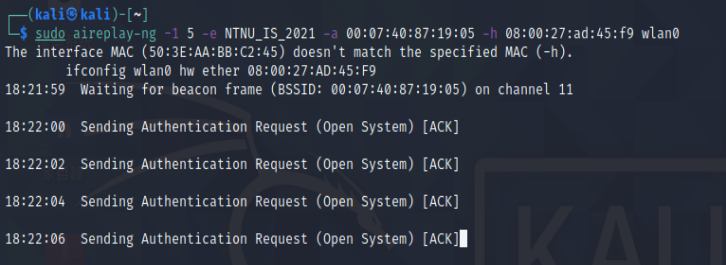
找尋附近的wifi，並找到目標MAC地址(BSSID)



針對要攻擊的WEP抓取封包並存到wep\_2021



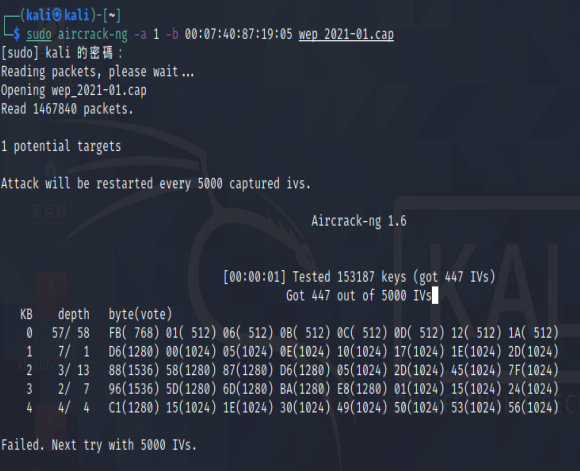




對該wifi進行Packet Injection，藉此獲取目標封包

參考網址:

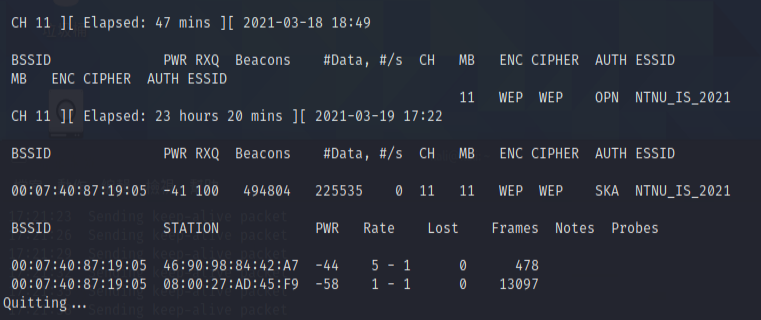
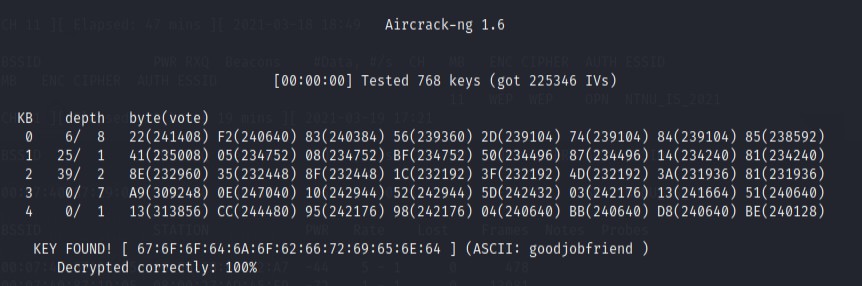
<http://atic-tw.blogspot.com/2014/01/aireplay-ng6.html>



透過內建字典庫對應抓取到的封包進行解密，上圖為接收到約450個封包後嘗試解密的結果。

最終結果:

密碼為goodjobfriend



放在pc4大約跑了22小時(3/19下午3點，後接收到的封包數量突然爆增，不然原本預計要跑到星期一的)

在收到20多萬個封包後，終於成功解出密碼。