4. Targeted Packet Sniffing

After scanning via airodump-ng you get like previous stated a similar output like this:

```
CH 2 ][ Elapsed: 18 s ][ 2018-10-08 09:59
BSSID
                                     #Data, #/s
                                                  CH
                                                       MB
                                                                  CIPHER AUTH ESSID
                    PWR
                         Beacons
                                                            ENC
64:16:F0:EC:7B:F3
                    -50
                               29
                                          0
                                               0
                                                   6
                                                       270
                                                            WPA
                                                                  CCMP
                                                                               Test AP
                                                                               eir21601582-2.4G
5C:A8:6A:16:A0:4C
                    -38
                               13
                                          2
                                               0
                                                    1
                                                       54e
                                                            WEP
                                                                  WEP
                    -50
                                          2
                                                   3
F8:23:B2:B9:50:A8
                               21
                                               0
                                                       130
                                                            OPN
                                                                               Eir88
F8:23:B2:B9:50:A9
                    -53
                               20
                                          0
                                               0
                                                    3
                                                       130
                                                            WPA2 CCMP
                                                                               eir WiFi
                                                                         MGT
BSSID
                    STATION
                                         PWR
                                               Rate
                                                        Lost
                                                                 Frames
                                                                         Probe
```

Pic a target network like shown in the ESSID

```
airodump-ng --bssid 11:22:33:44:55:55 --channel 5 --write ~/test-01 wlan0
```

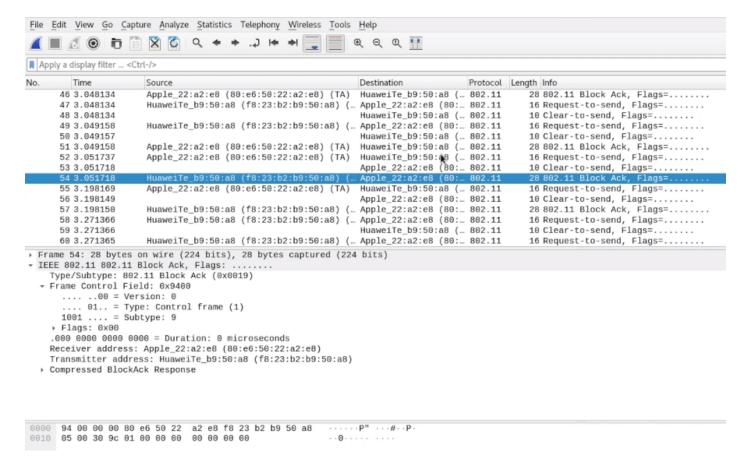
You will see someting like this:

```
CH 2 ][ Elapsed: 2 mins ][ 2018-10-08 10:27
BSSID
                   PWR RXQ Beacons
                                        #Data, #/s
                                                         MB
                                                    CH
                                                              ENC
                                                                   CIPHER AUTH ESSID
F8:23:B2:B9:50:A8
                   -47 52
                                1152
                                          161
                                                  1
                                                      2
                                                         130
                                                              WPA2 CCMP
                                                                           PSK eir73766789-2.4G
BSSID
                   STATION
                                       PWR
                                             Rate
                                                      Lost
                                                              Frames
                                                                      Probe
                                        -1
                                                                   2
                                               1e- 0
                                                          0
F8:23:B2:B9:50:A8
                   40:98:AD:98:51:70
F8:23:B2:B9:50:A8
                   80:E6:50:22:A2:E8
                                       -29
                                               0 -24e
                                                          0
                                                                 189
                                                                       Ţ
F8:23:B2:B9:50:A8
                   8C:BF:A6:E3:AC:58
                                       -54
                                                          0
                                                                  41
```

Now you'll get several cap files. The interesting one for now is .cap, which can be directly be opened in Wireshark

```
root@kali:~# ls
Desktop Downloads Pictures Templates test-01.csv test-01.kismet.netxml
Documents Music Public test-01.cap test-01.kismet.csv Videos
```

Wireshark:



This Packages are all encrypted. If the Wireless Network wouldn't use any encryption, we could see directly see all the URLs and probably passwords. However the example is encrypted and they also will be the foundation of up coming attacks

Revision #5 Created 10 February 2023 17:50:38 by tinfoil-hat Updated 9 March 2023 18:06:05 by tinfoil-hat