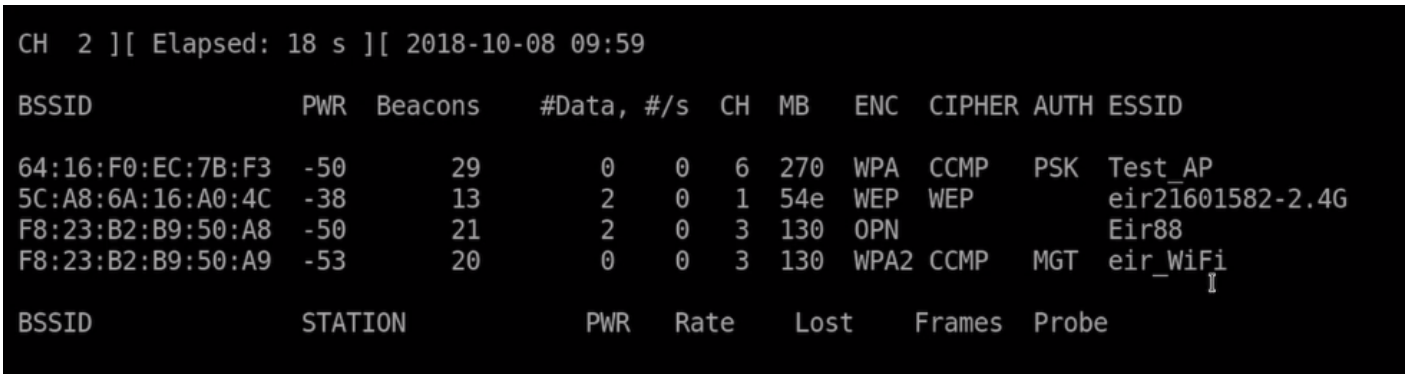
4. Targeted Packet Sniffing

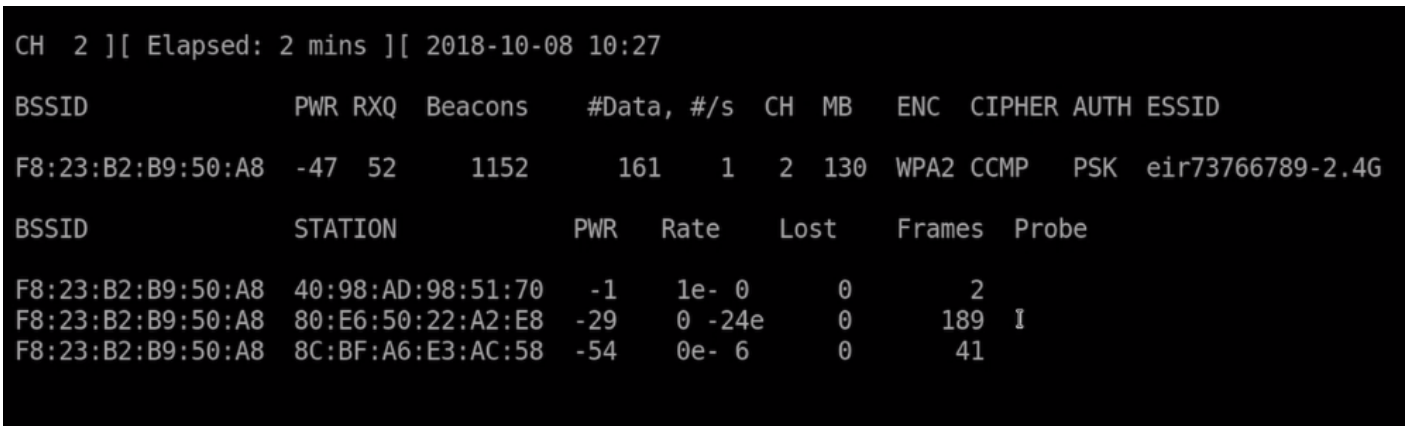
After scanning via airodump-ng you get like previous stated a similar output like this:



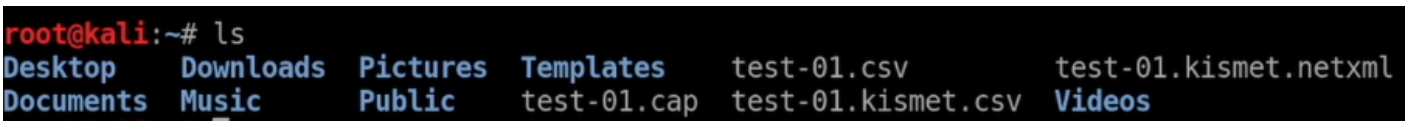
Pic a target network like shown in the ESSID

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

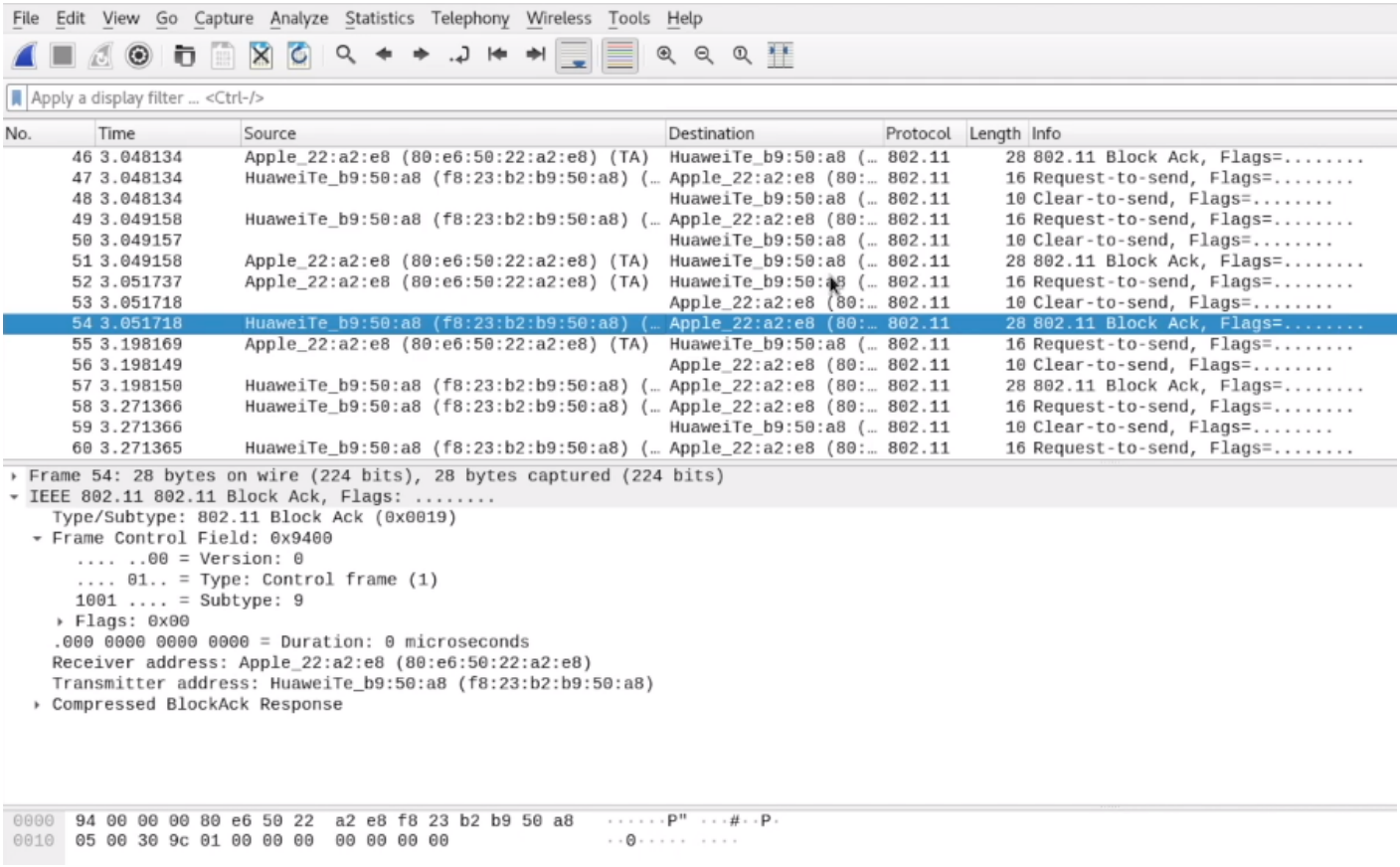
You will see someting like this:



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



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 2023-02-10 17:50:38 UTC by tinfoil-hat
Updated 2023-03-09 18:06:05 UTC by tinfoil-hat