wifi-stuf

Jacob Petrisko, Bailey Morgan, and Jake Zimmerman

Goals

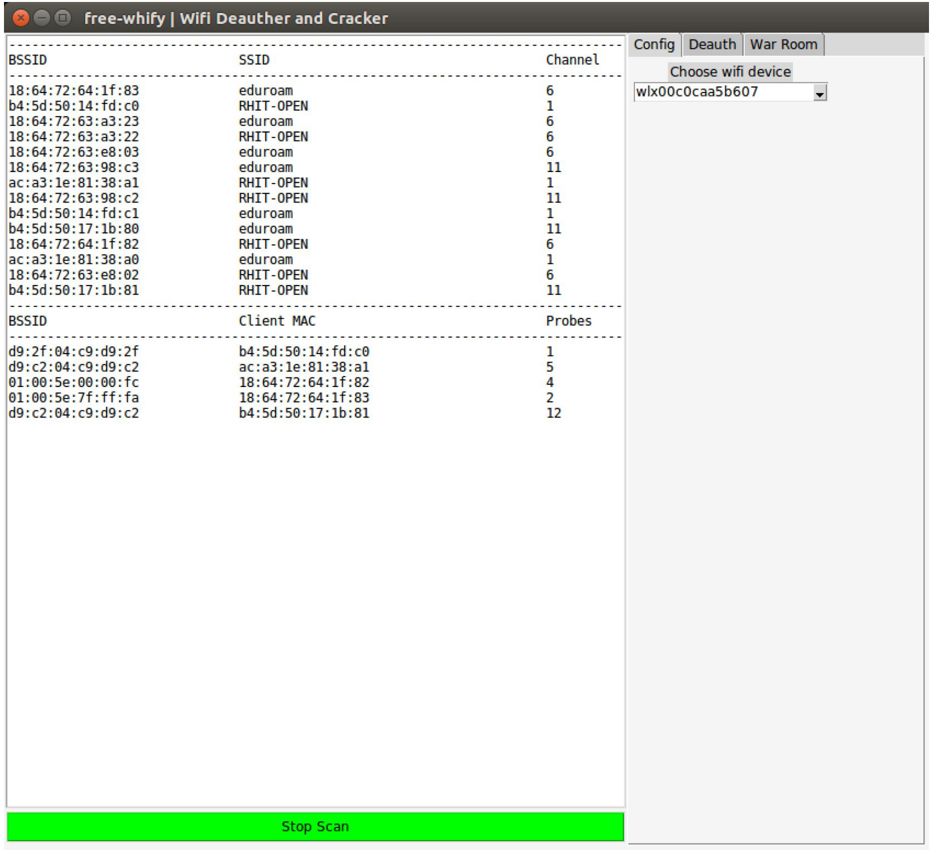
- Wifi Scanning
- Deauth Attacks
- WPA Brute-Forcing

Resources

- Python
- Tkinter
- Scapy (Networking)

GUI

- Tkinter
- Considered web based front end



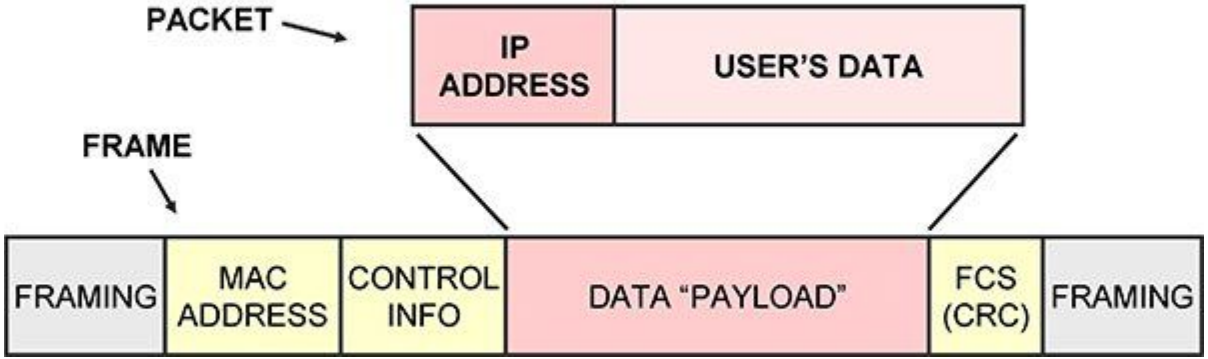
free-whify | Wifi Deauther and Cracker

```
----------------------------------------------------------------
BSSID                   SSID                            Channel
----------------------------------------------------------------
18:64:72:64:1f:83       eduroam                         6
b4:5d:50:14:fd:c0       RHIT-OPEN                       1
18:64:72:63:a3:23       eduroam                         6
18:64:72:63:a3:22       RHIT-OPEN                       6
18:64:72:63:e8:03       eduroam                         6
18:64:72:63:98:c3       eduroam                         11
ac:a3:1e:81:38:a1       RHIT-OPEN                       1
18:64:72:63:98:c2       RHIT-OPEN                       11
b4:5d:50:14:fd:c1       eduroam                         1
b4:5d:50:17:1b:80       eduroam                         11
18:64:72:64:1f:82       RHIT-OPEN                       6
ac:a3:1e:81:38:a0       eduroam                         1
18:64:72:63:e8:02       RHIT-OPEN                       6
b4:5d:50:17:1b:81       RHIT-OPEN                       11
----------------------------------------------------------------
BSSID                   Client MAC                      Probes
----------------------------------------------------------------
d9:2f:04:c9:d9:2f       b4:5d:50:14:fd:c0               1
d9:c2:04:c9:d9:c2       ac:a3:1e:81:38:a1               5
01:00:5e:00:00:fc       18:64:72:64:1f:82               4
01:00:5e:7f:ff:fa       18:64:72:64:1f:83               2
d9:c2:04:c9:d9:c2       b4:5d:50:17:1b:81               12
```

Choose wifi device: wlx00c0caa5b607

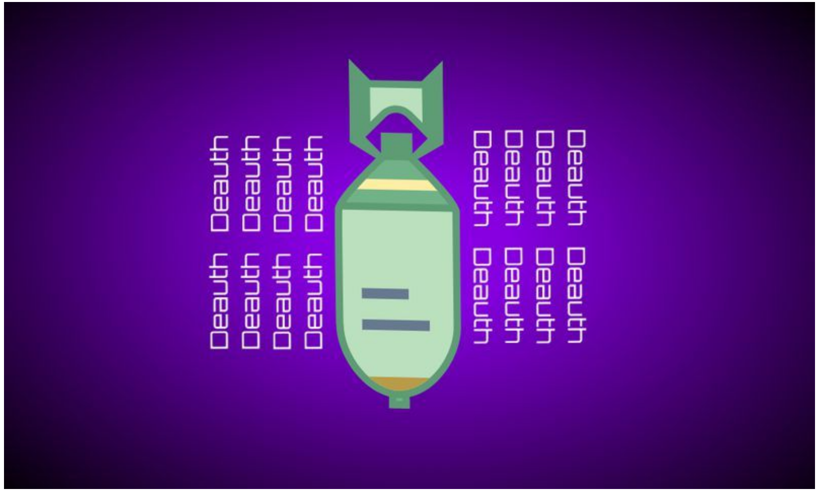
Networking with Scapy

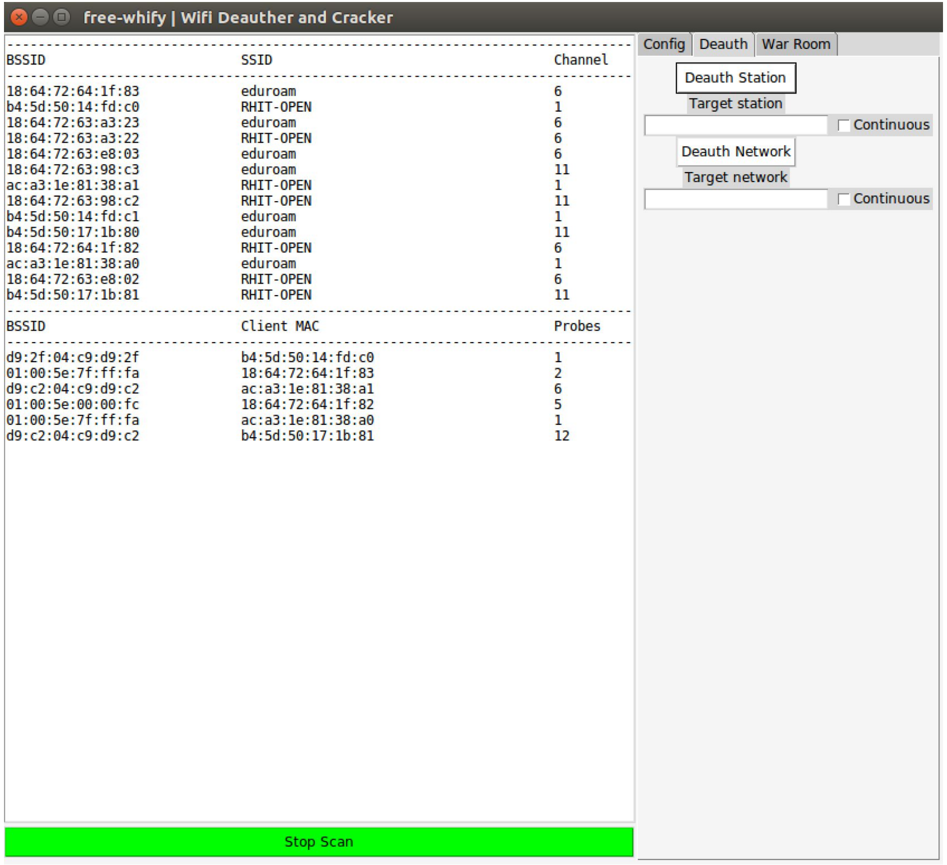
- Scapy works at the physical layer
- Can view and inject MAC frames



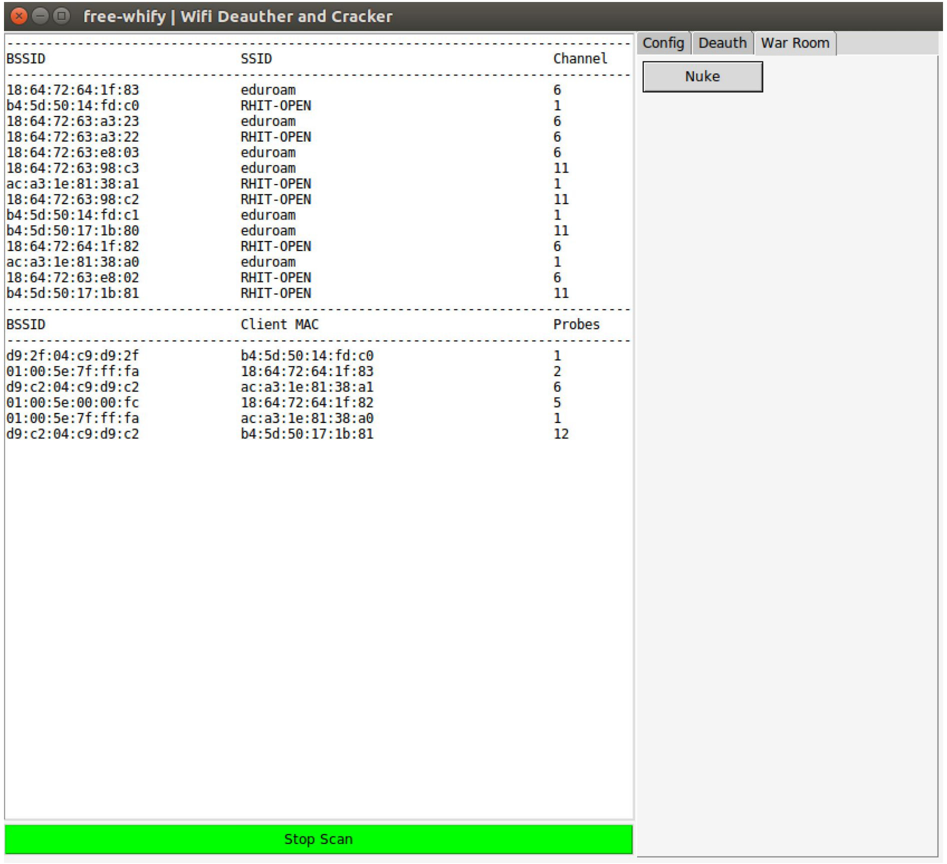
Deauth Attacks

- Types
  - Single client
  - Specific access point
  - Every access point in range (Nuclear)





```
----------------------------------------------------------------
BSSID                 SSID                    Channel
----------------------------------------------------------------
18:64:72:64:1f:83     eduroam                 6
b4:5d:50:14:fd:c0     RHIT-OPEN               1
18:64:72:63:a3:23     eduroam                 6
18:64:72:63:a3:22     RHIT-OPEN               6
18:64:72:63:e8:03     eduroam                 6
18:64:72:63:98:c3     eduroam                 11
ac:a3:1e:81:38:a1     RHIT-OPEN               1
18:64:72:63:98:c2     RHIT-OPEN               11
b4:5d:50:14:fd:c1     eduroam                 1
b4:5d:50:17:1b:80     eduroam                 11
18:64:72:64:1f:82     RHIT-OPEN               6
ac:a3:1e:81:38:a0     eduroam                 1
18:64:72:63:e8:02     RHIT-OPEN               6
b4:5d:50:17:1b:81     RHIT-OPEN               11
----------------------------------------------------------------
BSSID                 Client MAC              Probes
----------------------------------------------------------------
d9:2f:04:c9:d9:2f     b4:5d:50:14:fd:c0       1
01:00:5e:7f:ff:fa     18:64:72:64:1f:83       2
d9:c2:04:c9:d9:c2     ac:a3:1e:81:38:a1       6
01:00:5e:00:00:fc     18:64:72:64:1f:82       5
01:00:5e:7f:ff:fa     ac:a3:1e:81:38:a0       1
d9:c2:04:c9:d9:c2     b4:5d:50:17:1b:81       12
```



```
----------------------------------------------------------------
BSSID                 SSID                    Channel
----------------------------------------------------------------
18:64:72:64:1f:83     eduroam                 6
b4:5d:50:14:fd:c0     RHIT-OPEN               1
18:64:72:63:a3:23     eduroam                 6
18:64:72:63:a3:22     RHIT-OPEN               6
18:64:72:63:e8:03     eduroam                 6
18:64:72:63:98:c3     eduroam                 11
ac:a3:1e:81:38:a1     RHIT-OPEN               1
18:64:72:63:98:c2     RHIT-OPEN               11
b4:5d:50:14:fd:c1     eduroam                 1
b4:5d:50:17:1b:80     eduroam                 11
18:64:72:64:1f:82     RHIT-OPEN               6
ac:a3:1e:81:38:a0     eduroam                 1
18:64:72:63:e8:02     RHIT-OPEN               6
b4:5d:50:17:1b:81     RHIT-OPEN               11
----------------------------------------------------------------
BSSID                 Client MAC              Probes
----------------------------------------------------------------
d9:2f:04:c9:d9:2f     b4:5d:50:14:fd:c0       1
01:00:5e:7f:ff:fa     18:64:72:64:1f:83       2
d9:c2:04:c9:d9:c2     ac:a3:1e:81:38:a1       6
01:00:5e:00:00:fc     18:64:72:64:1f:82       5
01:00:5e:7f:ff:fa     ac:a3:1e:81:38:a0       1
d9:c2:04:c9:d9:c2     b4:5d:50:17:1b:81       12
```

Deauth attacks on clients and access points (left) and for everything (right)

Hacking WPA

- Capture WPA authentication handshake
- Run a dictionary attack against it
- Half finished this

Demo

Questions?