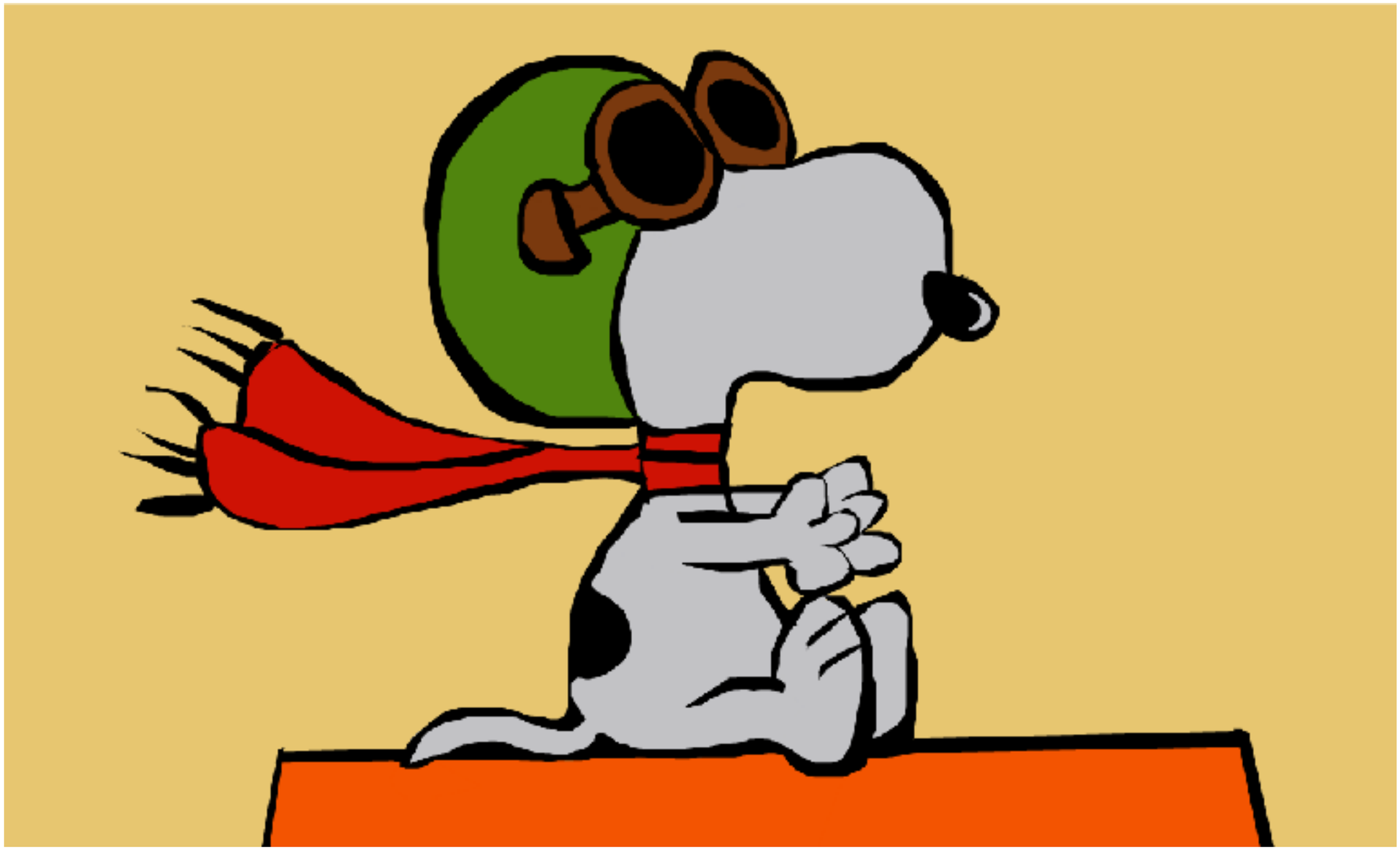

# snoopy-ng

modular digital terrestrial tracking framework

# The story so far

- We can passively intercept MACs and SSIDs by monitoring wifi traffic
- This can be augmented with data from public databases
- This combination could allow tracking devices (and their owners)
- Doing this with Wireshark is incredibly tedious

| Source | SSID |
|---|---|
| Apple_56:[redacted] | ViTo1337@Home |
| Apple_56:[redacted] | UPC17852AE |
| Apple_56:[redacted] | ChristiansAP3 |
| Apple_56:[redacted] | UPC17852AE |
| Apple_56:[redacted] | FRITZ!Box 6490 Cable |
| Apple_56:[redacted] | PC-Notdienst-Office |
| Apple_56:[redacted] | Unitymedia Store Kassel dez |
| Apple_56:[redacted] | FRITZ!Box 6490 Cable |
| Apple_56:[redacted] | Unitymedia Store Kassel dez |
| Apple_56:[redacted] | ViTo1337@Home |
| Apple_56:[redacted] | Koalasoft |
| Apple_56:[redacted] | PC-Notdienst-Office |
| Apple_56:[redacted] | Unitymedia Store Kassel dez |
| Apple_56:[redacted] | FRITZ!Box 6490 Cable |
| Apple_56:[redacted] | ViTo1337@Home |
| Apple_56:[redacted] | Unitymedia Store Kassel dez |
| Apple_56:[redacted] | ViTo1337@Home |
| Apple_56:[redacted] | ViTo1337@Home |
| Apple_56:[redacted] | UPC17852AE |
| Apple_56:[redacted] | Koalasoft |
| Apple_56:[redacted] | PC-Notdienst-Office |
| Apple_56:[redacted] | Unitymedia Store Kassel dez |
| Apple_56:[redacted] | FRITZ!Box 6490 Cable |
| Apple_56:[redacted] | ChristiansAP3 |

# Enter sensepost/snoopy-ng

- Simple application that logs information to a database
- Written in Python
- Client-Server
- Comes with an import-filter for Maltego
- Relatively simple to extend with new plugins
- Runs nicely on a Raspberry

# The bad news

- Snoopy is dead
- To my knowledge no comparable tool exists
- Some bitrot has already happened

# The good news

- Snoopy is opensource
- The code is simple enough
- The core components are unaffected

# So what can it do?

- Data-gathering:
  – Wifi (Advertisements, Probes, Handshakes, Cookies)
  – Bluetooth (discoverable devices)
  – GPS (the drones position)
  – RogueAP (not useful by itself)
  – MitM (broken?)

- Augmentation:
  – WiGLE (locations for SSIDs)

- Architectural:
  – Server (receives data from drones and other servers)
  – Local Sync (syncs data with a server)

- Misc: Heartbeat, Sysinfo

# Not a Demo

- Server:

```
$ snoopy_auth --create myDrone
$ snoopy -m server -m wigle:username=<user>,password=<pass>,email=<mail>
```

- Drone:

```
$ snoopy -m wifi:mon=True,iface=wlan1 -m gpsd -m sysinfo -m heartbeat \
        -s http://server:9001 -d myDrone -l meetup -k <key>
```

- Client:

```
$ snoopy -m local_sync:server_url=http://server_ip:9001 -d myDrone -k <key>
```

# Now what?

- The gathered data can be imported into Maltego
- Maltego is a tool for analyzing directed graphs
- Devices become nodes, connections become edges
- Maltego CE comes free with Kali

# That’s all folks

(but not really)