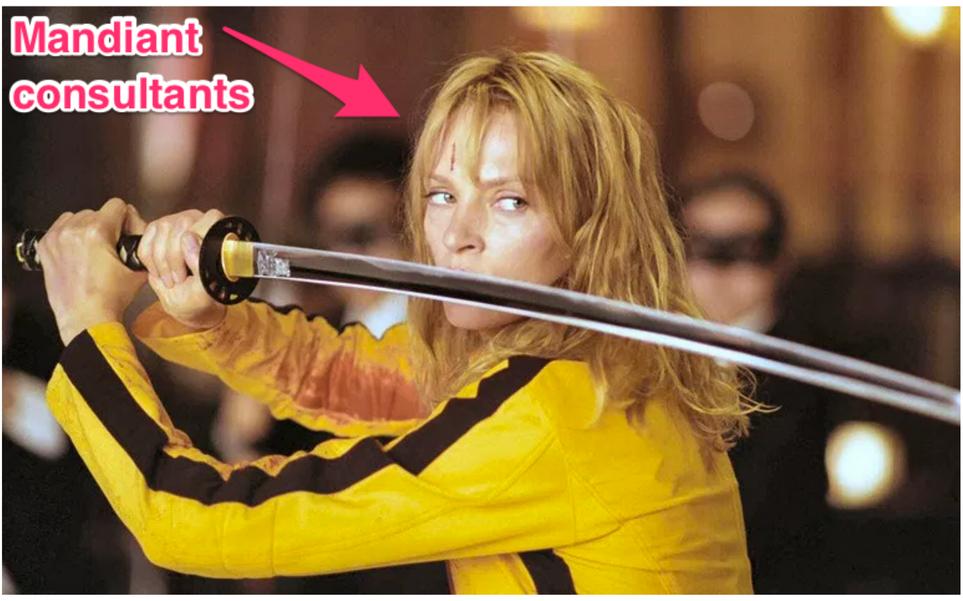
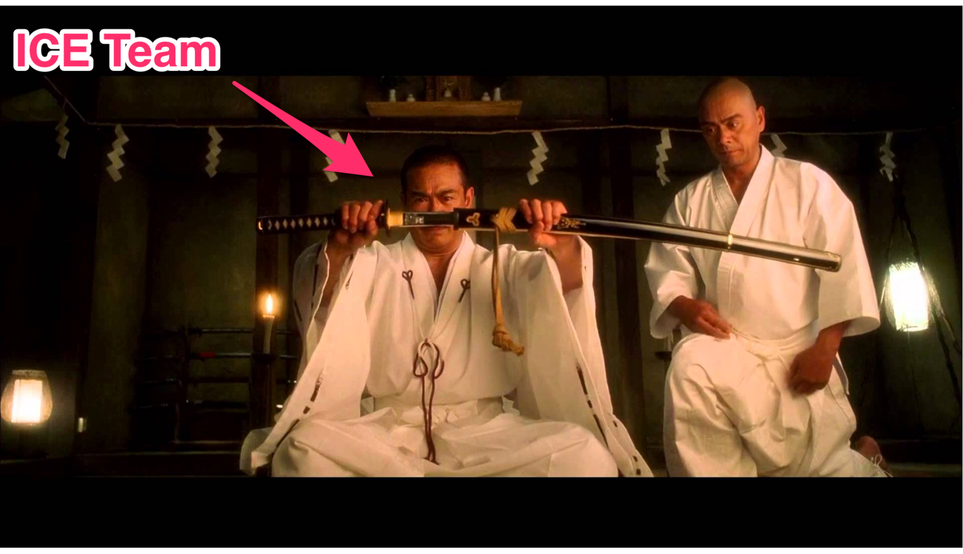
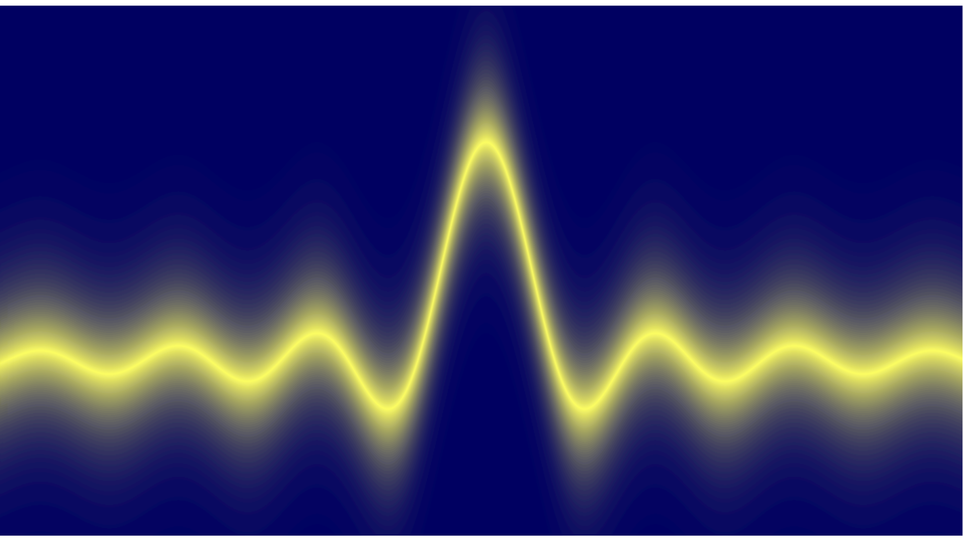
mapping wifi networks and triggering on interesting traffic patterns

Caleb Madrigal
Website: http://calebmadrigal.com/
Twitter: @caleb_madrigal
Ham call sign: w0hak





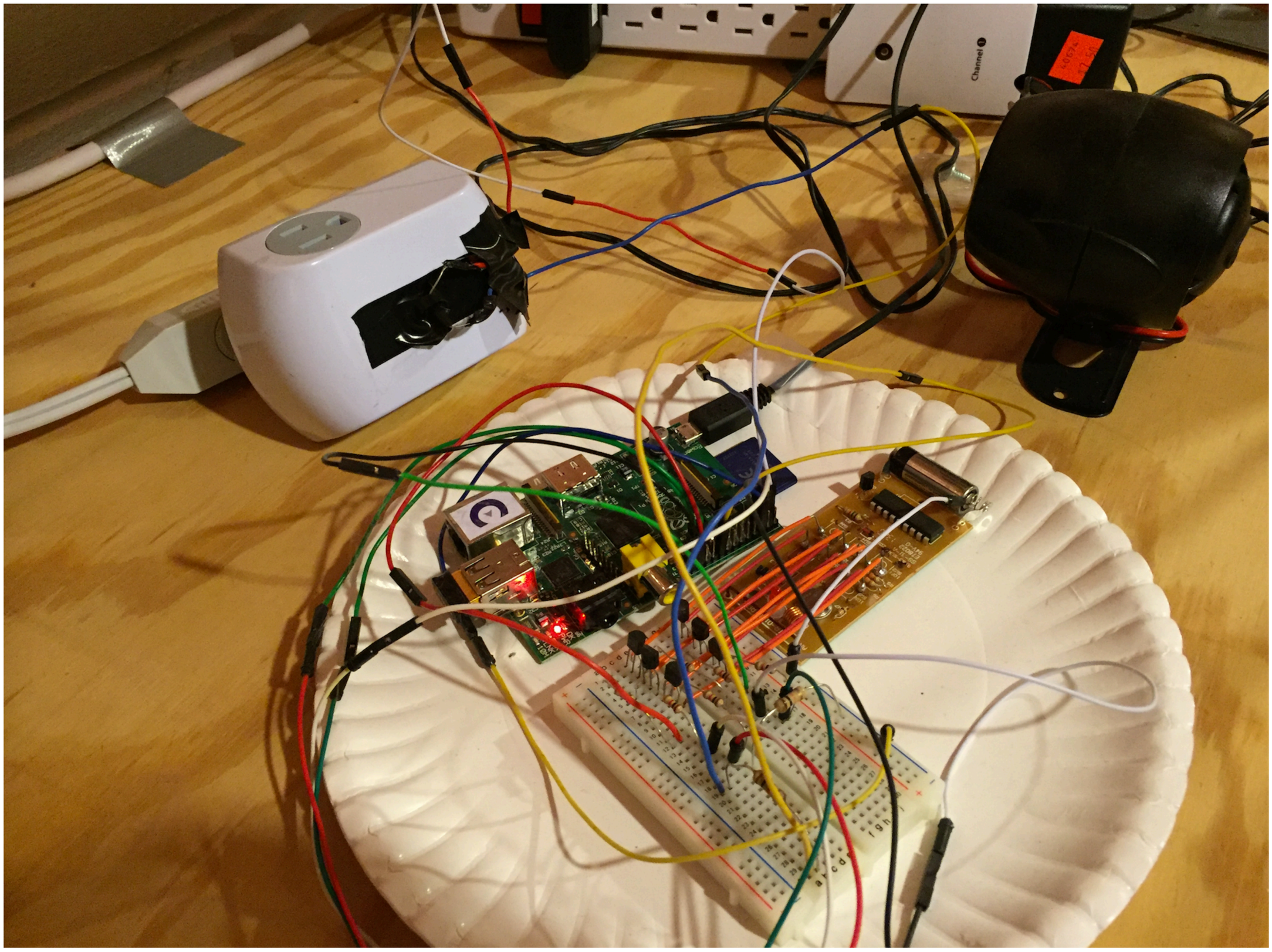
I like fuzzy things



(Generated on https://truthygraph.github.io/)


HAWKINS

I was into "IoT" before I knew it was called IoT



(http://calebmadrigal.com/raspberry-pi-home-security-system/)

Wireless hacking is really interesting

OSI Model

Data	*Layer*
Data	**Application** Network Process to Application
Data	**Presentation** Data Representation and Encryption
Data	**Session** Interhost Communication
Segments	**Transport** End-to-End Connections and Reliability
Packets	**Network** Path Determination and IP (Logical Addressing)
Frames	**Data Link** MAC and LLC (Physical Addressing)
Bits	**Physical** Media, Signal, and Binary Transmission

Host Layers

Media Layers

OSI Layer 4/3 (TCP/IP packets): Fun stuff, but less fun with ssl
OSI Layer 1 (802.11 modulation): Suddenly accessible with SDR
OSI Layer 2 (802.11 data frames): Data link - Less fun with good, ubiquitous wireless encryption (**boring ! ?**)

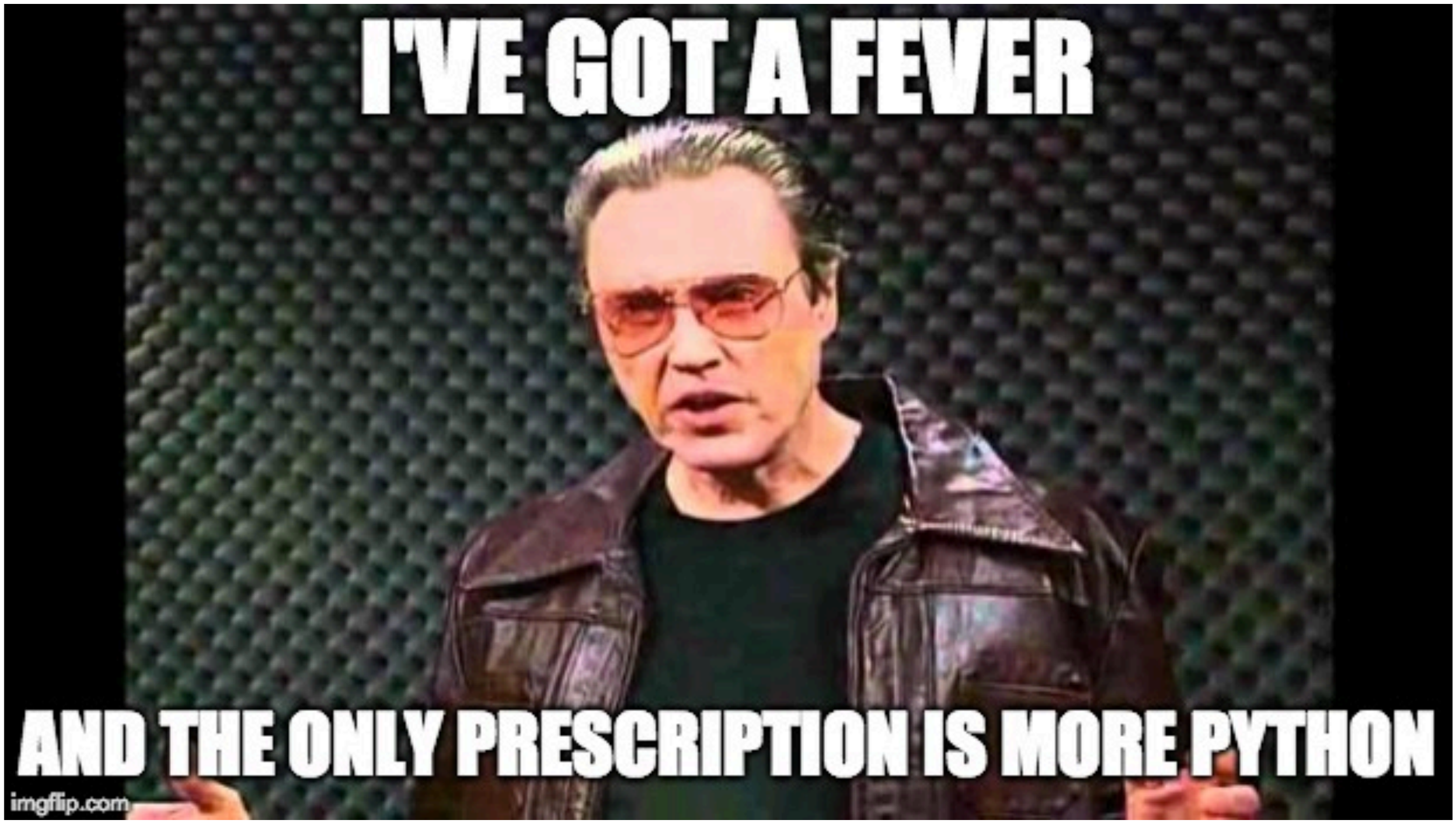
802.11 - Data Link Layer (OSI layer 2) data

- Explicit data in data frames
    - Source MAC
    - Destination MAC
    - Network SSID and BSSID (MAC)
    - Frame type (management, data, etc)
    - Encrypted data :(

802.11 - Data Link Layer (OSI layer 2) data

- Explicit data in data frames
    - Source MAC
    - Destination MAC
    - Network SSID and BSSID (MAC)
    - Frame type (management, data, etc)
    - Encrypted data
- Inferred data
    - Power level
    - Time
    - Manufacturer (via IEEE OUI)
    - Network/SSID (not always present, but inferable from history)

I had a problem...


I'VE GOT A FEVER
AND THE ONLY PRESCRIPTION IS MORE PYTHON
imgflip.com


the solution?
trackerjacker

trackerjacker

- https://github.com/calebmadrigal/trackerjacker
- https://pypi.python.org/pypi/trackerjacker
- Install: **pip3 install trackerjacker**

Demo 1: Inferring Wireless Camera Motion Detection

- Video

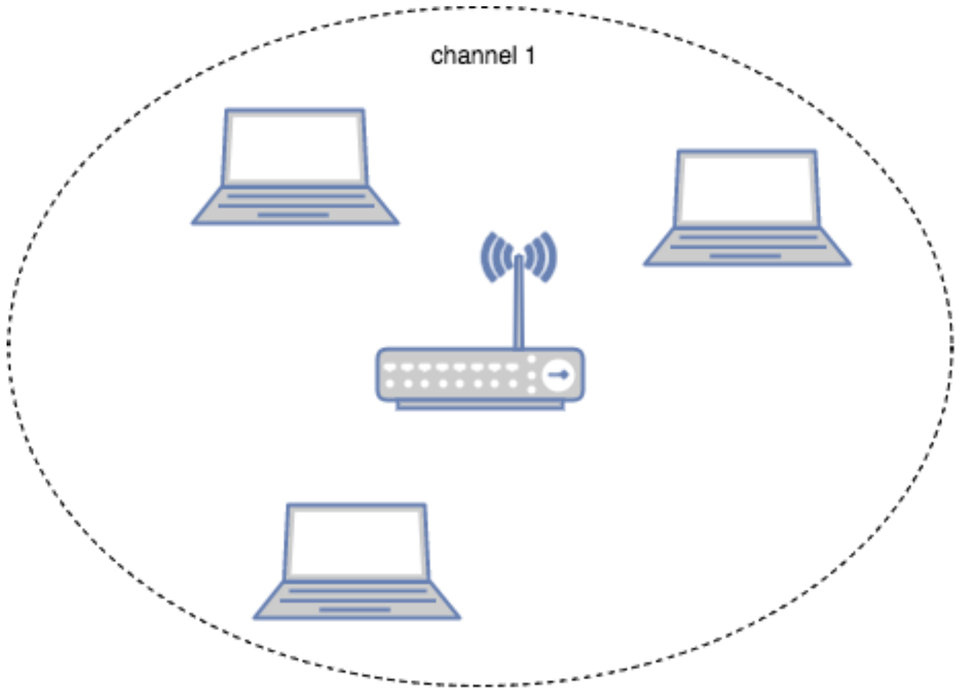
Demo 2: Tracking smartphones

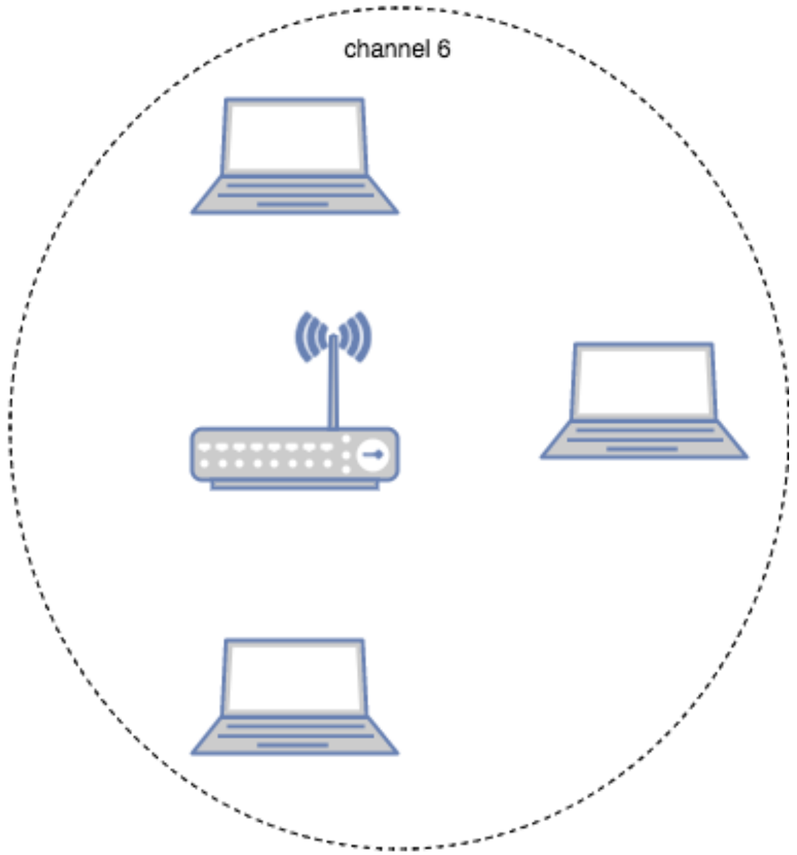
- trackerjacker --track -m 3c:2e:ff:25:30:61 --log-level=DEBUG --channel-switch-scheme=round_robin

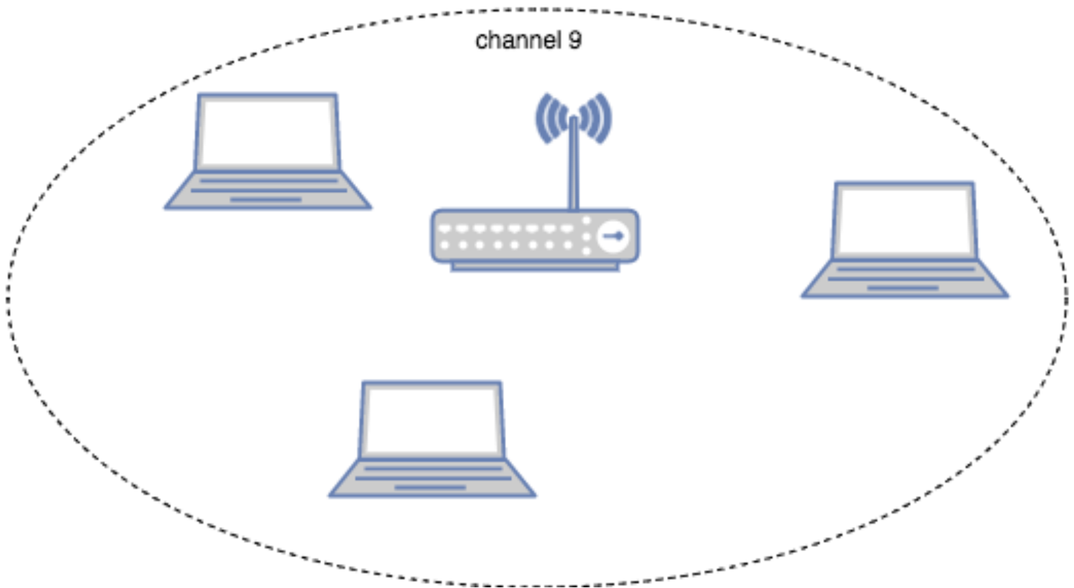
Demo 3: Mapping

- trackerjacker --map

How wifi works (from a radio perspective)





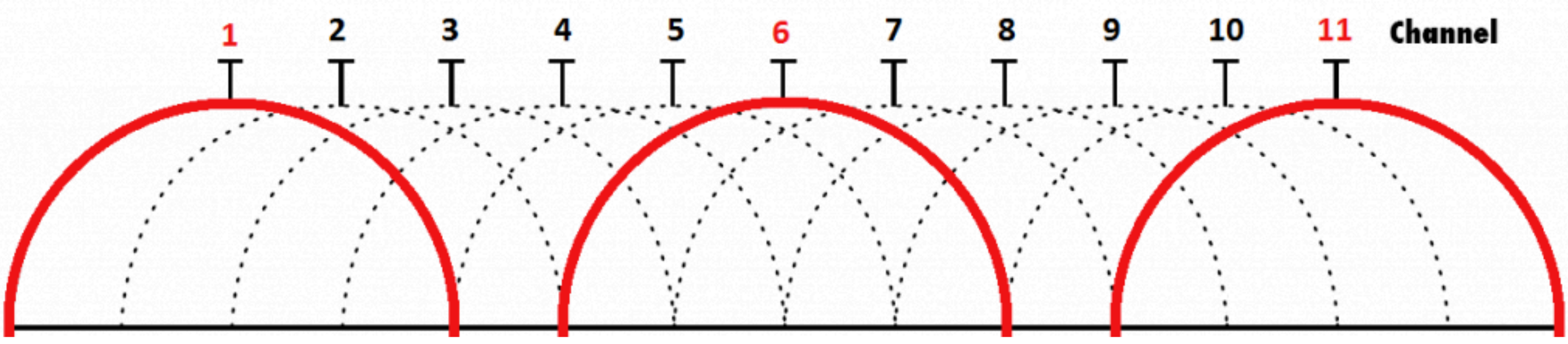


2.4 GHz Channels

CHANNEL NUMBER	LOWER FREQUENCY MHZ	CENTER FREQUENCY MHZ	UPPER FREQUENCY MHZ
1	2401	2412	2423
2	2406	2417	2428
3	2411	2422	2433
4	2416	2427	2438
5	2421	2432	2443
6	2426	2437	2448
7	2431	2442	2453
8	2436	2447	2458
9	2441	2452	2463
10	2446	2457	2468
11	2451	2462	2473
12	2456	2467	2478
13	2461	2472	2483
14	2473	2484	2495

5 GHz Channels

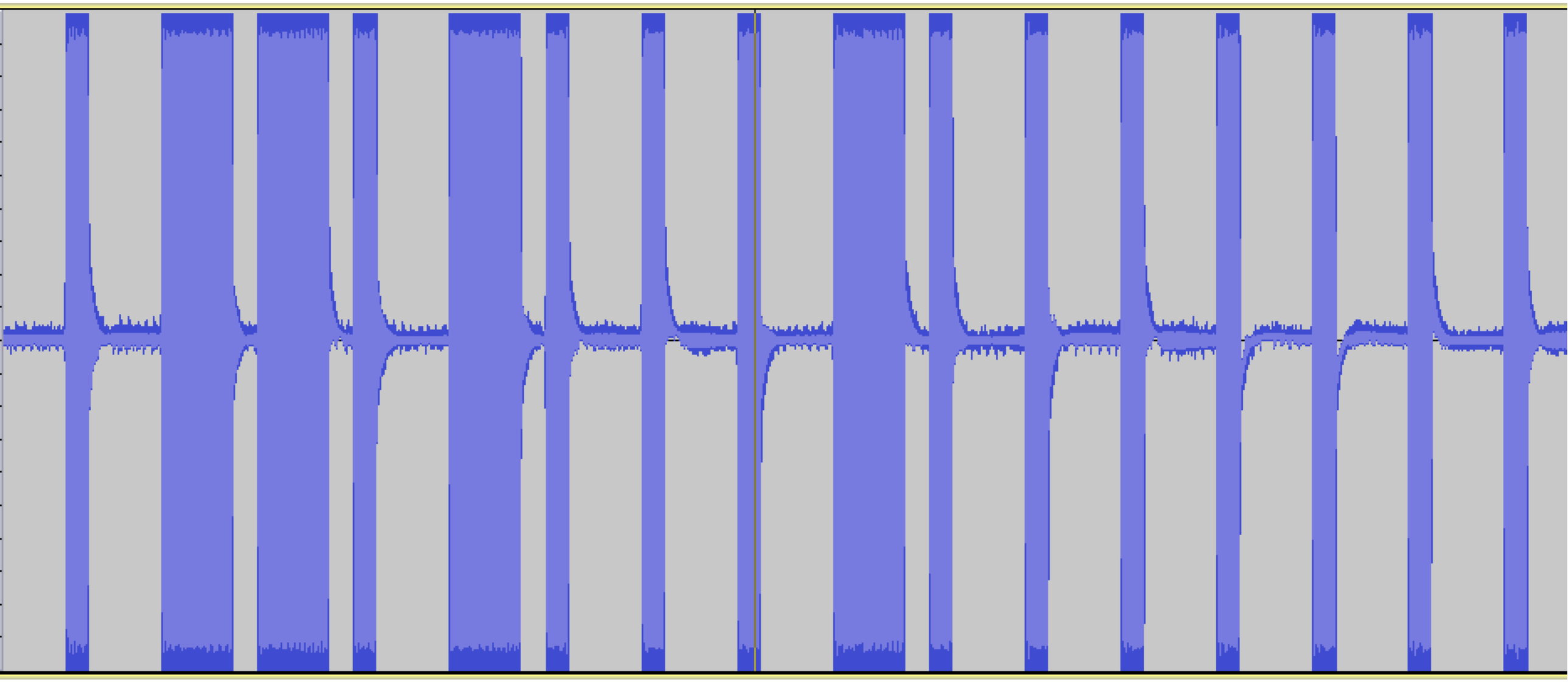
CHANNEL NUMBER	FREQUENCY MHZ
36	5180
40	5200
44	5220
48	5240
52	5260
56	5280
60	5300
64	5320
100	5500
104	5520
108	5540
112	5560
116	5580
120	5600
124	5620
128	5640
132	5660
136	5680
140	5700
149	5745
153	5765
157	5785
161	5805
165	5825



2.4 GHz (802.11b/g/n)

5 GHz (802.11a/n/ac)

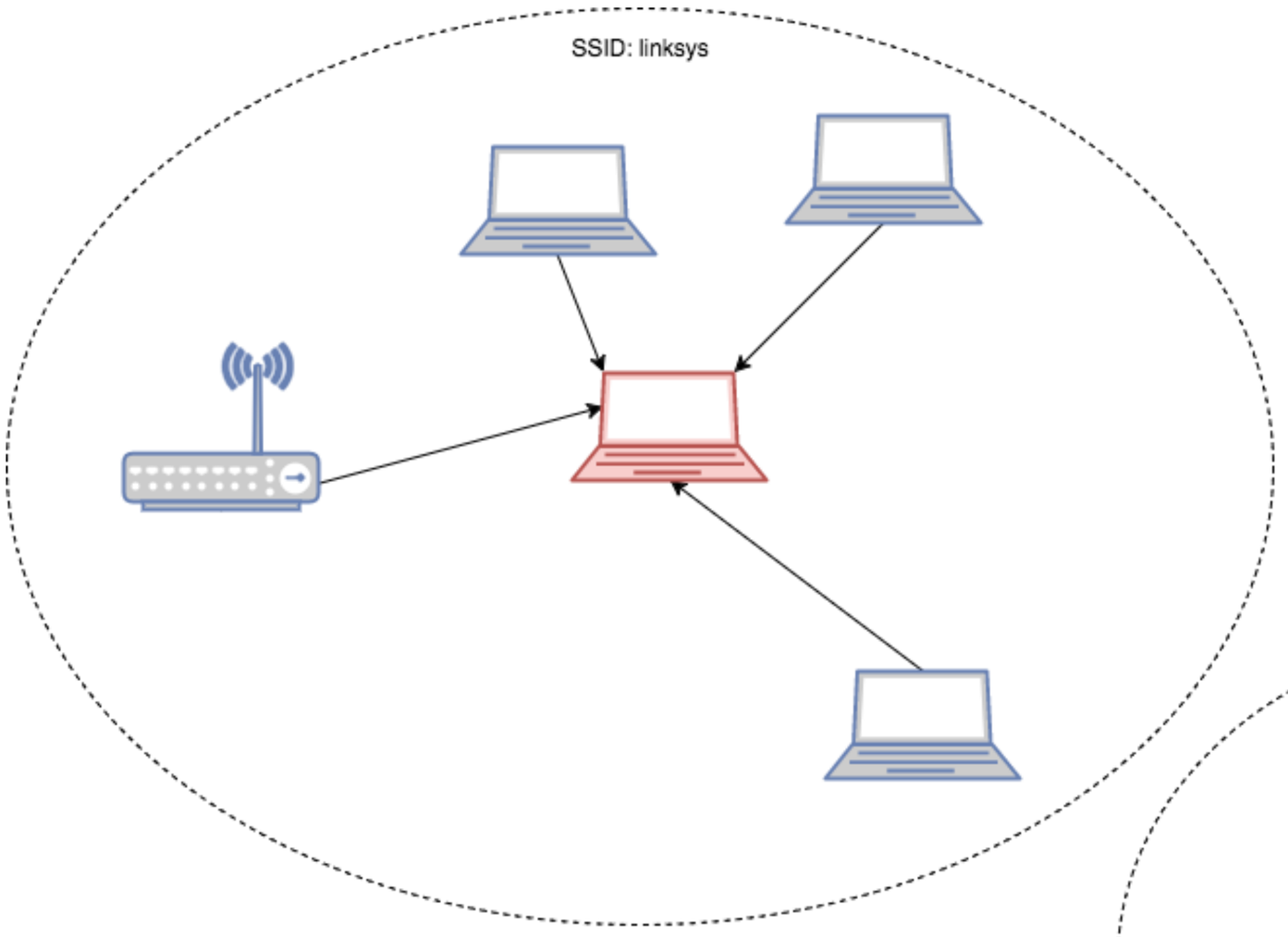
Modulation

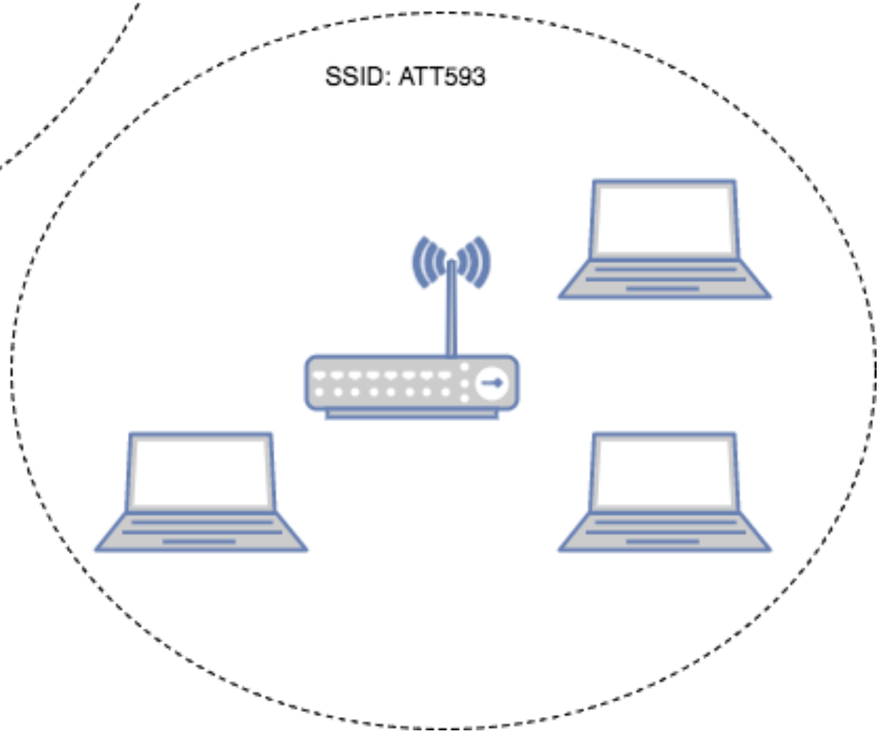


(http://calebmadrigal.com/digital-radio-signal-generation/, Note: this is a sample of ASK, whereas wireless typically uses FSK, PSK, or QAM)

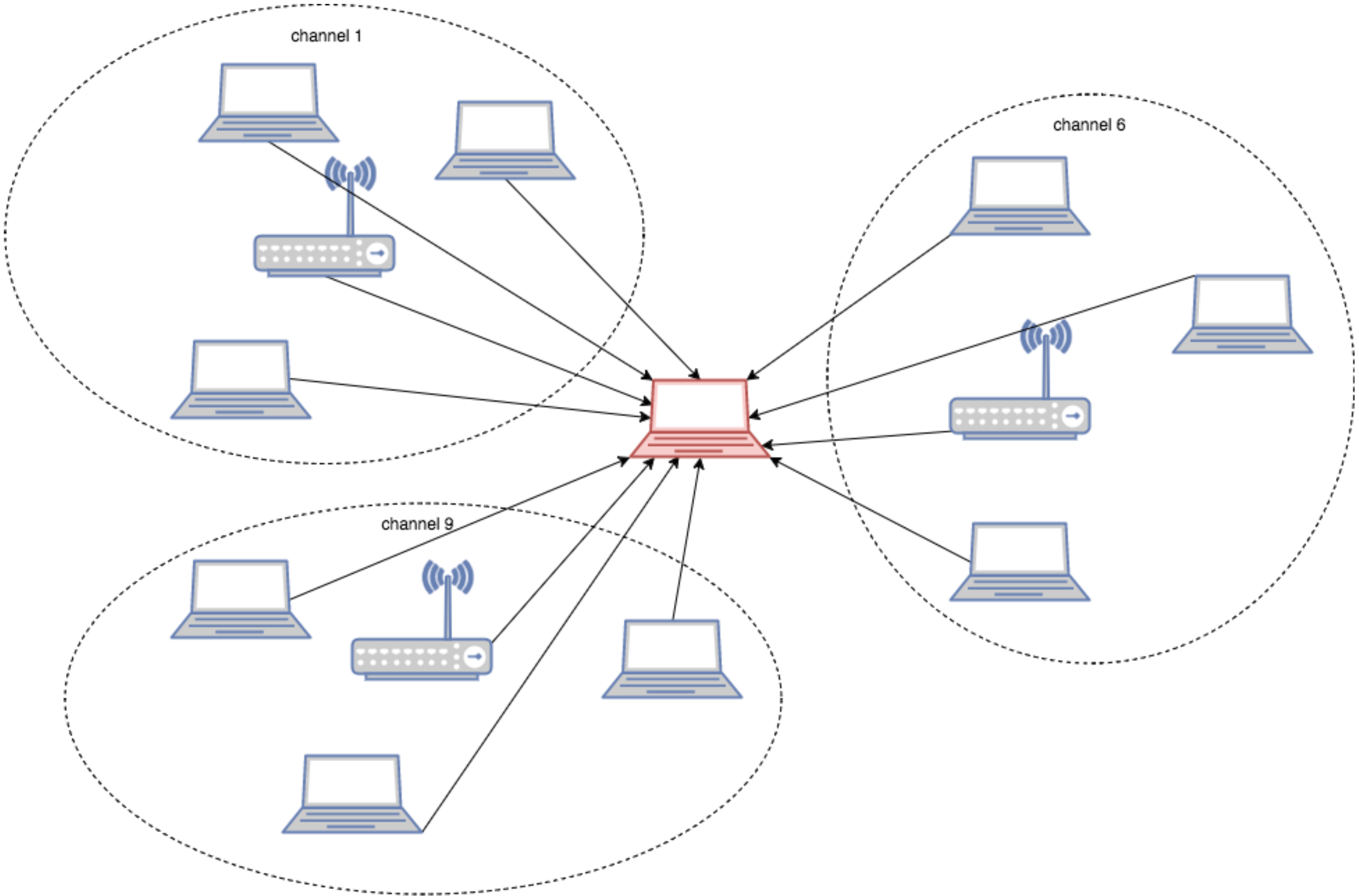
Monitor vs Promiscuous mode

Promiscuous mode





Monitor mode



Demo: foxhunt plugin

- trackerjacker --track --plugin foxhunt
- https://github.com/calebmadrigal/trackerjacker/blob/master/trackerjacker/plugins/foxhunt.py

Demo: deauth plugin

- trackerjacker --track --plugin plugin_examples/deauth_attack.py --plugin-config "{'vendor_to_deauth': 'Apple'}"
- https://github.com/calebmadrigal/trackerjacker/blob/master/plugin_examples/deauth_attack.py

Demo: example plugin

- trackerjacker --track --plugin plugin_examples/count_apples.py
- https://github.com/calebmadrigal/trackerjacker/blob/master/plugin_examples/count_apples.py

Environment

Recommendations

- Linux in a VM
    - I've also tested on Ubuntu
    - I've also tested in a Raspberry Pi
- An external wireless adapter
    - Especially if running in a VM
- macOS support is pre-alpha
    - (Don't bother reporting any bugs encountered in macOS)

Wireless Adapters

- Panda PAU07 N600 Dual Band (nice, small, 2.4GHz and 5GHz)
- Panda PAU09 N600 Dual Band (higher power, 2.4GHz and 5GHz)
- Alfa AWUS052NH Dual-Band 2x 5dBi (high power, 2.4GHz and 5GHz, large, ugly)
- TP-Link N150 (works well, but not dual band)

Panda Wireless

Panda N600 Dual Band (2.4GHz and 5.0GHz) 300Mbps Wireless N USB Adapter - Windows Vista/7/8/8.1/10, Mint, Ubuntu, openSUSE, Fedora, CentOS, Zorin, Kali Linux and Raspbian Jessie

4.2 out of 5 stars ▾ 343 customer reviews | 59 answered questions

Amazon's Choice for "panda wireless adapter"

- **Low Return Rate:** 43% fewer returns than similar products
- **Highly Rated:** 4.2 star rating with over 300 reviews
- **Popular Item:** Popular with customers shopping for "panda wireless adapter"

Price: $24.99 ✓prime | **FREE** One-Day

Get $40 off instantly: Pay $0.00 upon approval for the Amazon.com Store Card.

Take-away

- At the physical layer, wifi is just radio
- It is trivial to track Wifi devices with monitor mode
- Interesting information can be obtained just from the raw, encrypted 802.11 packets
    - Good to keep in mind with IoT stuff
- New tool: trackerjacker
- How to not be tracked: turn off wifi when not using (or use MAC randomization)

Thanks!

Questions?

Caleb Madrigal
Website: http://calebmadrigal.com/
Twitter: @caleb_madrigal
Ham call sign: w0hak
https://github.com/calebmadrigal/trackerjacker