Low cost, open source spectrum monitoring

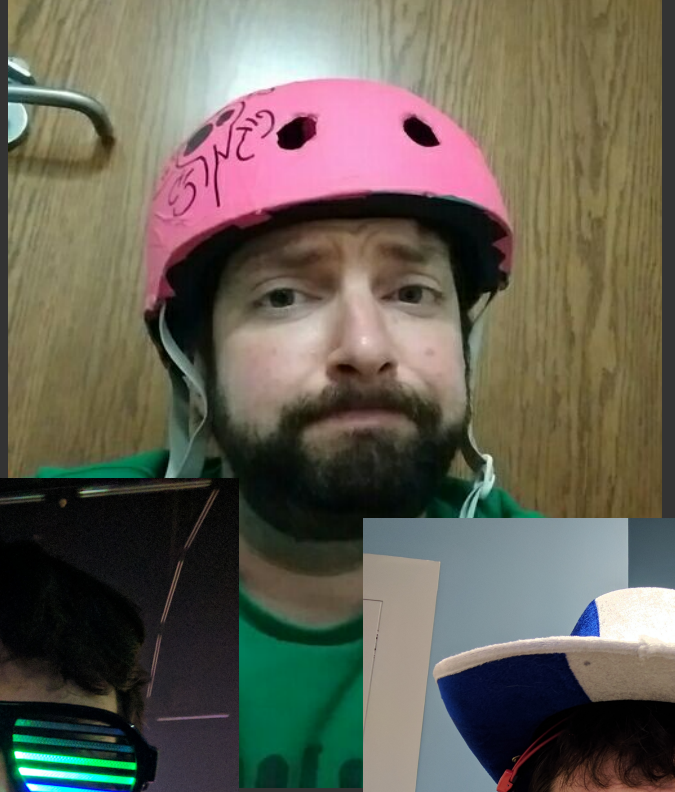
Dominic Spill
@dominicgs

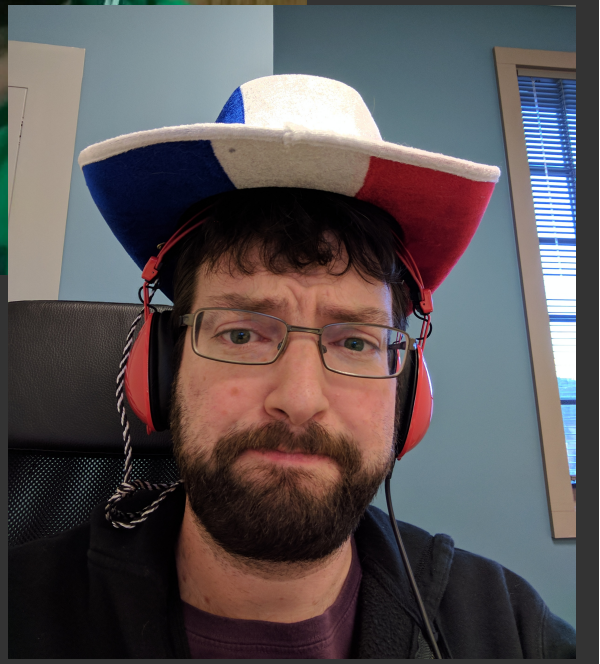
Great Scott Gadgets
@GSGlabs

HitB CommSec

Dominic Spill

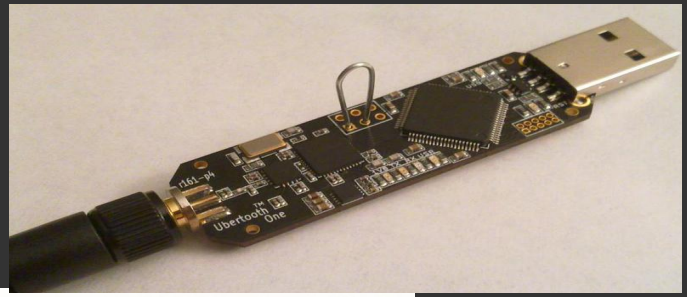
- Open source software developer
  - Ubertooth
  - GreatFET
  - HackRF
  - fcc.io

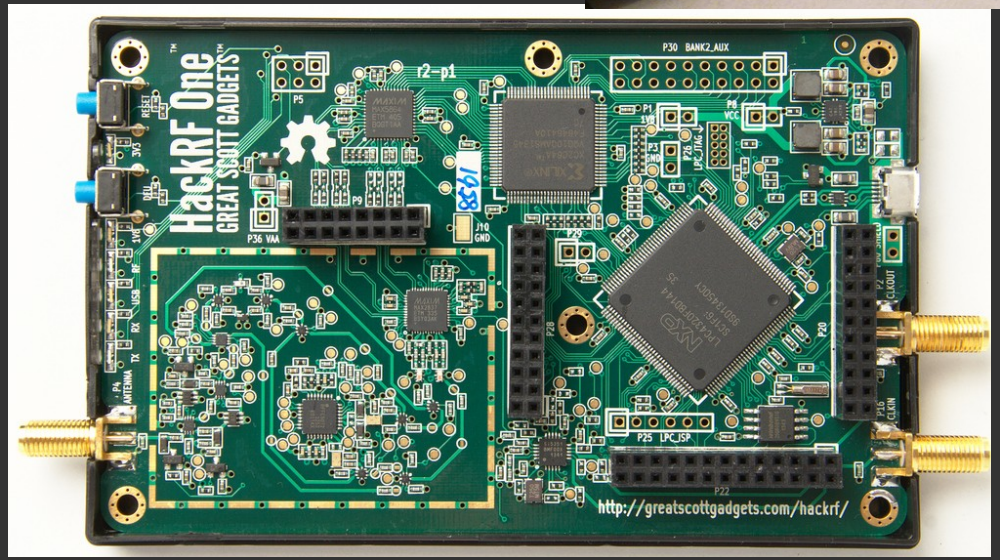


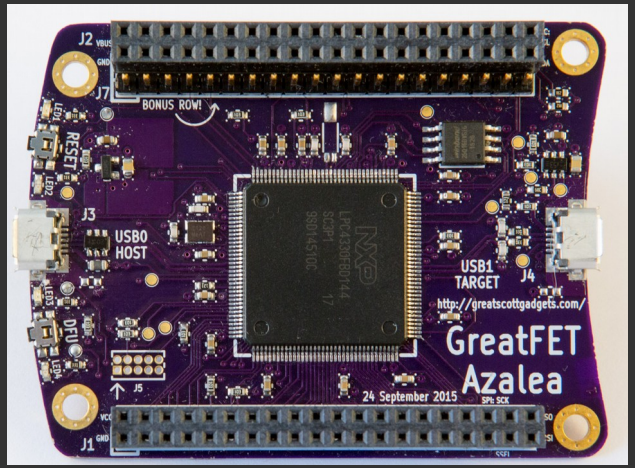


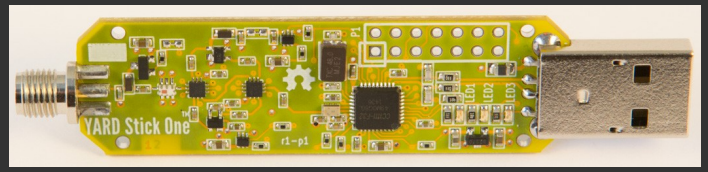
Great Scott Gadgets

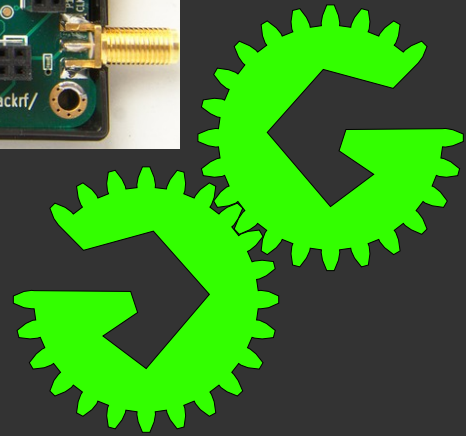
- HackRF One
- Ubertooth
- YARDStick One
- GreatFET











What is spectrum monitoring?

- Looking at the radio spectrum around us
- Finding and analyzing signals
- Identifying unknown transmitting devices

Who wants spectrum monitoring?

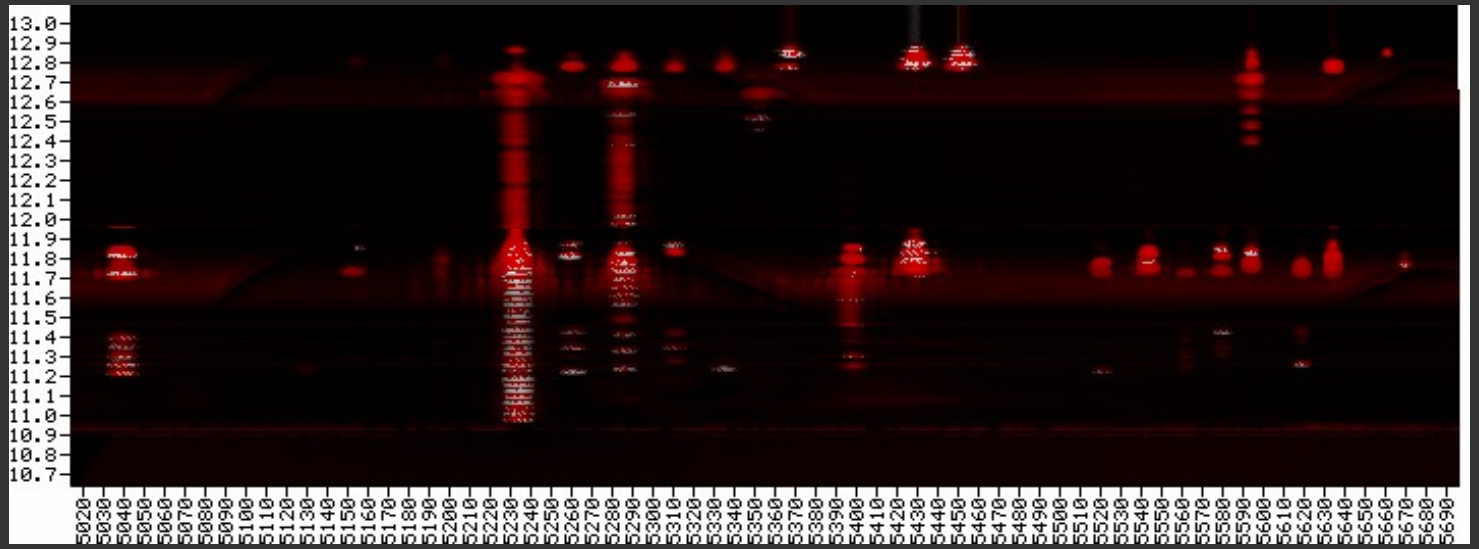
- Organisations
  - Protecting infrastructure
  - Knowing and controlling their environment
- Reverse engineers
  - Enumerating a device
- Hackers
  - Targets
- Radio Operators
  - Tracking down interference

How are we going to do it?

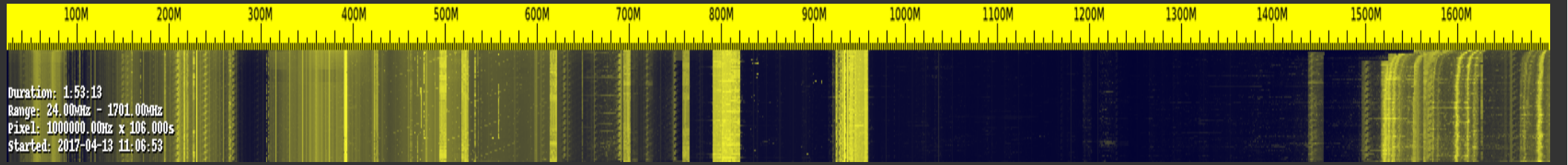
- Software Defined Radio
  - Rapidly tune radio
- FFT (Fast Fourier Transform)
  - Frequency to power map
- Plot frequency vs power
- Profit???

Plotting power vs frequency isn’t new

- Rtl-power + heatmap
  - kmkeen.com/rtl-power
- satmap
  - www.alcrypto.co.uk/satmap

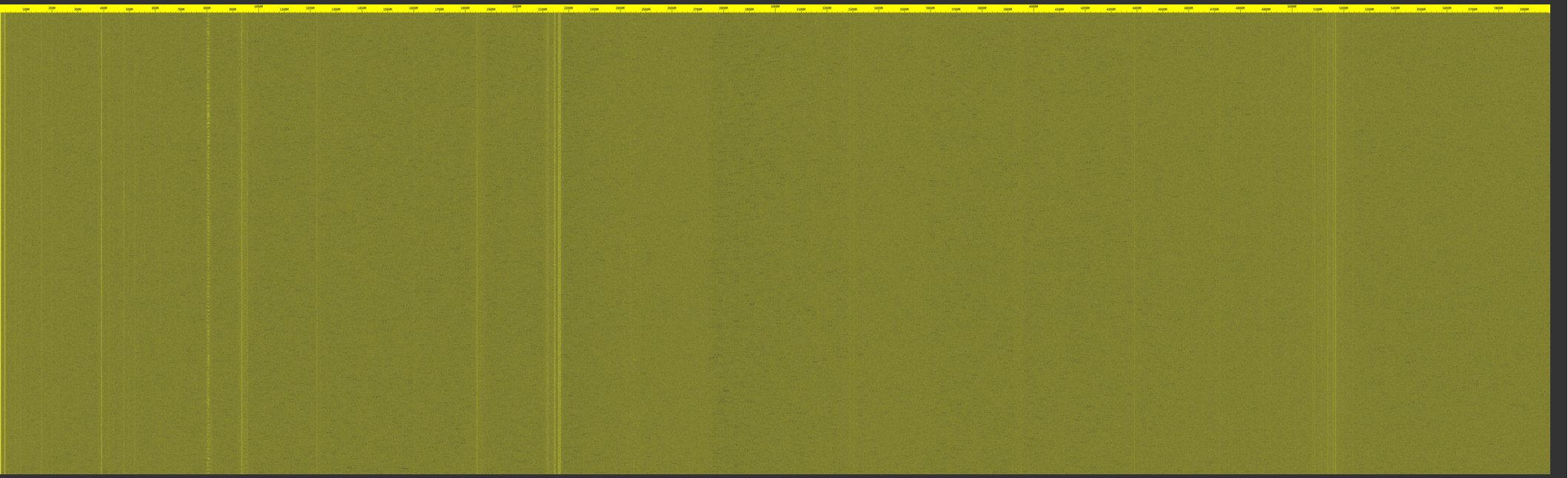


rtl_power + heatmap.py



hackrf_sweep + heatmap.py

hackrf_sweep + heatmap.py



Realtime visualization

- QspectrumAnalyzer
  - github.com/xmikos/qspectrumanalyzer

Inverse FFT

- Frequency:power map → samples
- Now we can use our favourite tools to view data

What’s next?

- Putting it all together
  - One tool to rule them all
  - nmap for RF
- Automation
  - Signal analysis
  - Signal Identification
- Direction finding
  - Pseudo Doppler

Thanks

- Great Scott Gadgets
  - Mike
  - Taylor
  - Elizabeth
- Mike Walters
  - @assortedhackery

Questions?

github.com/mossmann/HackRF

github.com/xmikos/qspectrumanalyzer

@dominicgs