All your RF belong to us;
Not just another RTL-SDR 101 talk

By: Gabe Thompson/@grnbeltwarrior

Disclaimer:

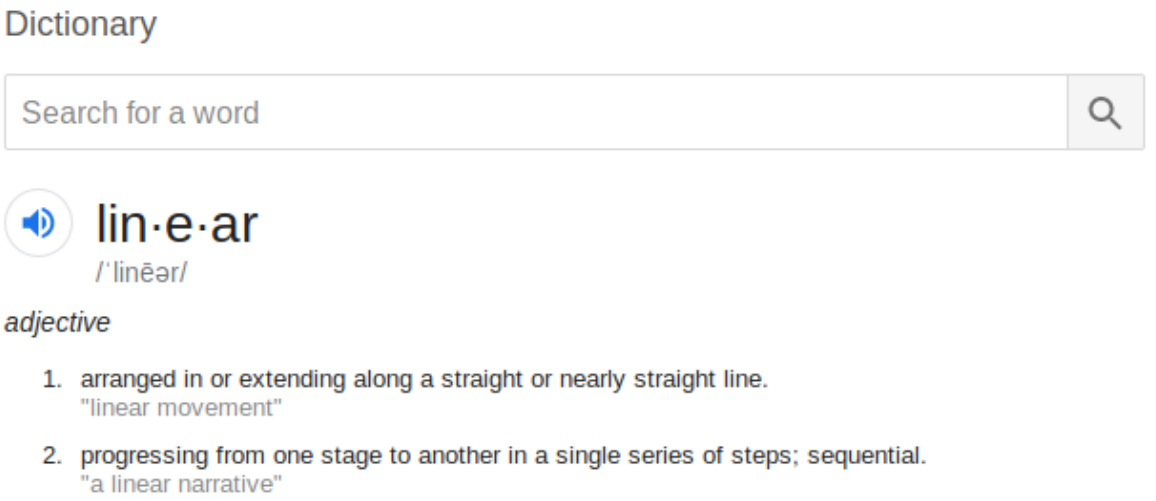
- FCC – Interception and Divulgence of Radio Communications
  - https://www.fcc.gov/consumers/guides/interception-and-divulgence-radio-communications
- Is there an expected level of privacy?
- With knowledge comes power, with power comes responsibility.
- I'm not a lawyer.
- All links are provided in my Medium Post that accompanies this talk. https://medium.com/@grnbeltwarrior

:~$ whoami

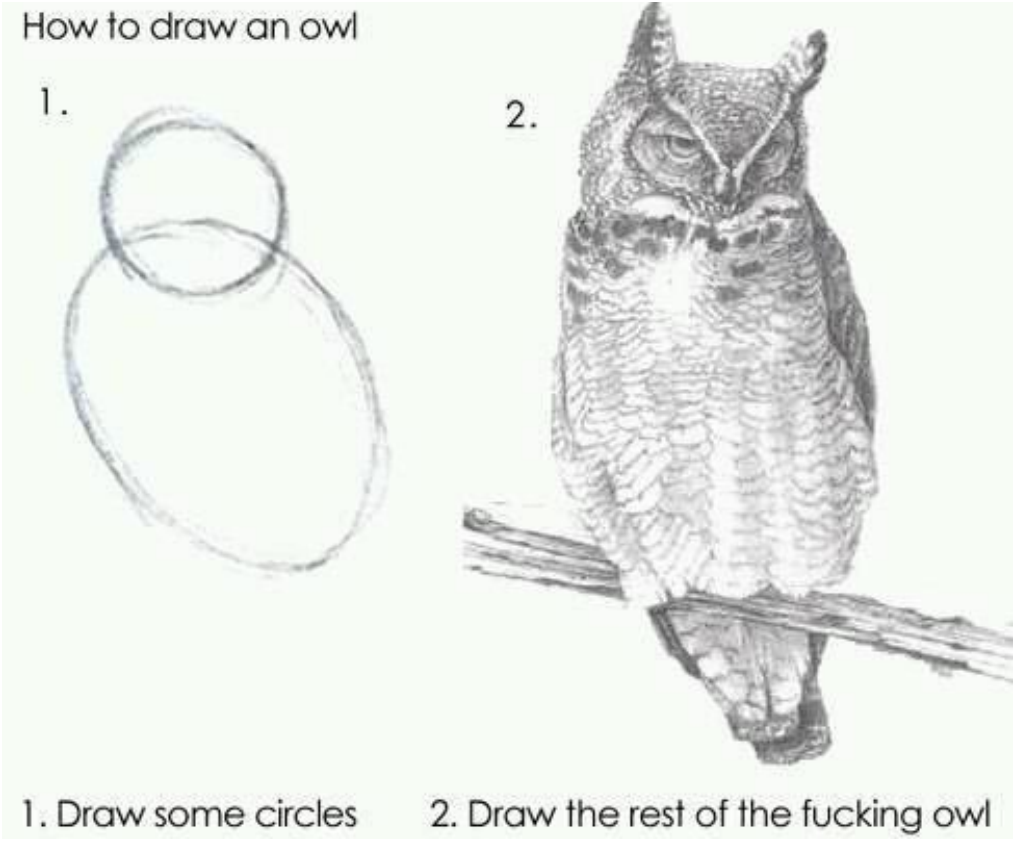
- Internal Penetration Tester for U.S. Bank
- Nearly a master's degree in Cybersecurity.
- Amateur radio license holder: KE0RHU
- Ultramarathon trail runner

:~ $ history

- Marine Corps
  - Firefighter
  - EMT
- Hazardous Material Disposal/Response Specialist
- Help Desk
- Desktop Support
- Network Administrator
- Technical Engineer
- Baseline and Vulnerability Scanning
- Penetration Testing



Hopefully not this...



What is this RF you speak of?

- Radio Frequency
- Generic term applied to oscillating electrical, magnetic or electromagnetic fields.
- Just like wireless, there is a lot of “stuff” in the air you can’t see or hear, with normal means.

Why this talk?

- Defcon 26 Wireless CTF.
  - Able to find a number of frequencies but lacked understanding of how to decode.
- POCSAG and FLEX still popular and interesting details found within.
- Vapor Trail – Data Exfiltration via Faraday's Law & Ponies
  - Larry Pesce and Galen Alderson
  - https://youtu.be/MM8WVZkhuy4
- Wireless exfiltration with SDR is possible.
  - https://www.blackhillsinfosec.com/webcast-building-a-small-and-flexible-wireless-exfiltration-box-with-sdr/

A Brief Tip Toe through the Tulips

- There are better and more thorough RTL-SDR videos/talks.
- Hitting the tops of the trees.

Basic Hardware

- Pros:
  - Cheap ($20)
- Cons:
  - Cheap (frequency drift as the chip heats up)

Better Basic Hardware

- Pros:
  - Inexpensive ($25-$30)
  - Better antenna options
- Cons:
  - Higher cost if you're not going to use it

Increasing the investment:

HackRF One: ~ $300
Half duplex RX and TX

BladeRF 2.0: ~$480
Full duplex RX and TX

Pentoo Plug

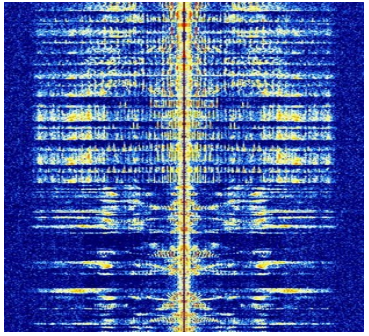
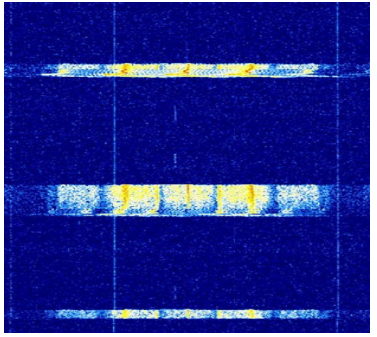
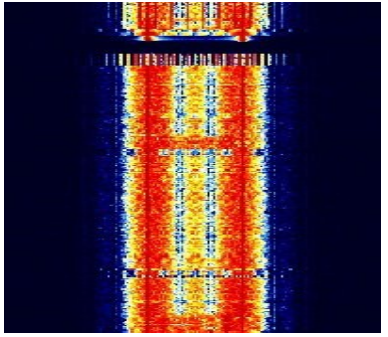
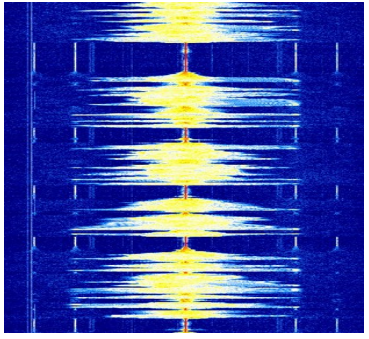
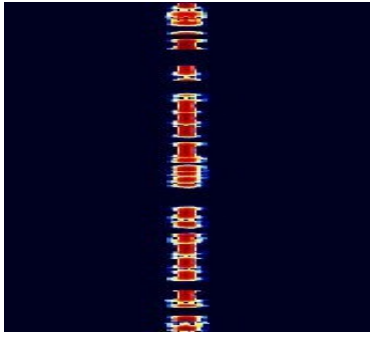
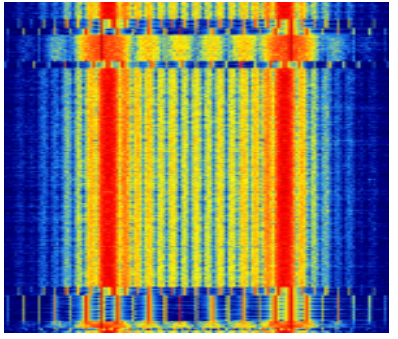
- Maintained by ZeroChaos, member of the wireless CTF team.
- Designed to work specifically with wireless/RF
- Especially the issues with drivers

- Gentoo based
- Will add a level of learning if you’re a Debian fan.
- Live boot or install it on a USB drive or locally.

Software

- gqrx
  - Based on gnuradio
  - Basic waterfall and plot.
  - Save as wav, playback and UDP streaming.
- gnuradio
  - Python based
  - Rapid custom development
  - Filters, demodulators, decoders and others.
- sdr#
  - Windows
  - Decent driver support
  - Personally, limited experience.

Signals

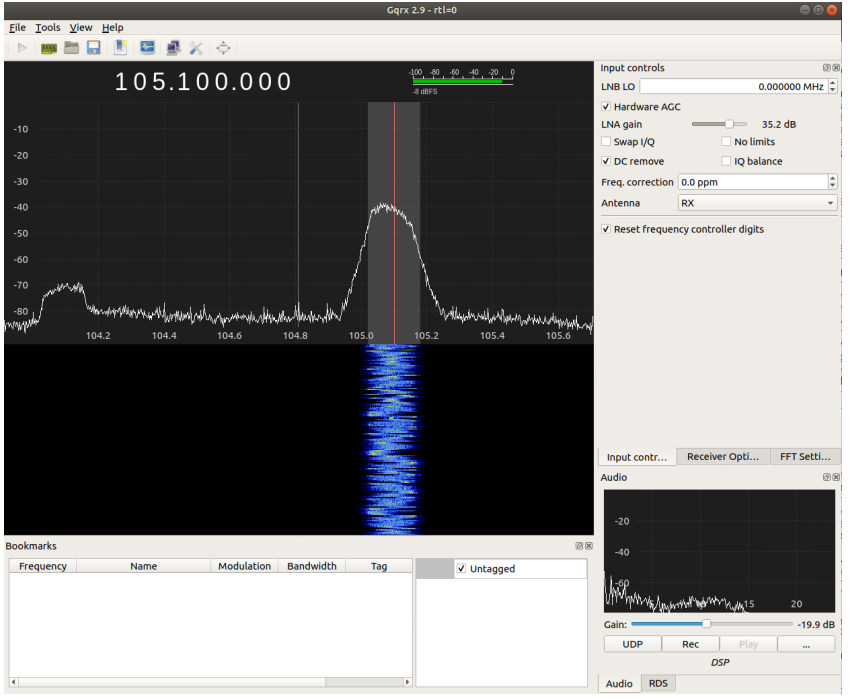







Sigidwiki.com

- https://www.sigidwiki.com/wiki/Signal_Identification_Guide
- Examples of signals to include waterfalls and audio recordings.

./gqrx

- Support for numerous SDR hardware.
- A lot of features (corrections, demodulators, record and streaming).
- Support on Linux and Raspberry Pi.
- http://gqrx.dk/doc/practical-tricks-and-tips#more-229



What is FLEX and POCSAG

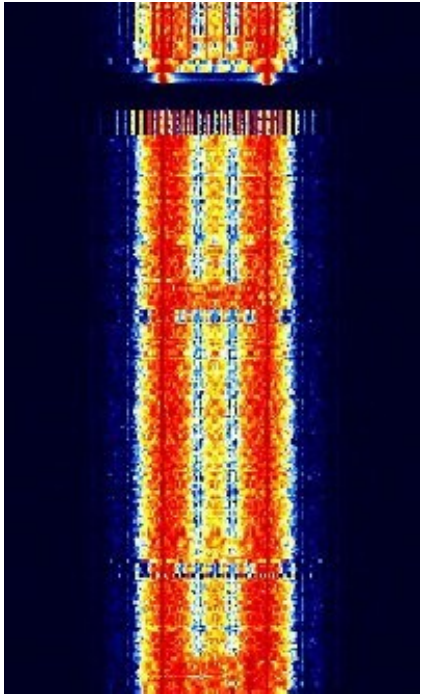
- FLEX
  - Flexible Wide Area Paging Protocol.
  - Motorola
  - 1 way paging.
  - A number of bits per second supported. 1600, 3200, and 6400.
- POCSAG
  - Post Office Code Standardization Advisory Group
  - British Post Office
  - 1 way paging.
  - A number of bits per second supported. 512, 1200, and 2400.

Identifying FLEX/POCSAG

- Double signal tracks.
- Similar to rails.
-
  - 152.6 MHz
  - 169 MHz
  - 309.505 MHz
  - 310.905 MHz
  - 929.362 MHz
  - 929.387 MHz
  - 929.538 MHz
  - 929.612 MHz
  - 929.662 MHz
  - 929.937 MHz

POCSAG Frequency Ranges

Paging Band	Frequency Range
HF-High/VHF-Low Band	25 MHz - 54 MHz
VHF Mid Band	66 MHz - 88 MHz
VHF High Band	138 MHz- 175 MHz
UHF	406 MHz - 422 MHz
UHF High	435 MHz - 512 MHz
'900' Band	929 MHz - 932 MHz



Decoding

- Using gqrx to output to UDP.
- Using netcat and chaining sox and multimon-ng.
- Use man pages to really learn the options of sox and multimon-ng.

- nc -lup 7355 |
- sox -t raw -esigned-integer -b 16 -r 48000 - -esigned-integer -b 16 -r 22050 -t raw - |
- multimon-ng -t raw -a FLEX -a POCSAG512 -a POCSAG1200 -a POCSAG2400 -f alpha -
- https://www.bastibl.net/pocsag/

Reading the output:

- FLEX: 2019-07-05 14:48:14 1600/4/C/A 12.016 [4294961352] ALN IS IS A TEST PERIODIC PAGE SEQUENTIAL NUMBER 8406N1/
- POCSAG512: Address: 425321 Function: 3 Alpha: GRAND CENTRAL<LF><LF>HACKRF THE

Demos

- Strong signals can cause interference on other frequencies.
- The size of your antenna matters but not in the way you might believe.
- While the information that can be gathered from this process is traveling around us, using the information for malicious intent isn’t something we should be doing.

POCSAG and FLEX?

- Let’s take a look in gqrx.

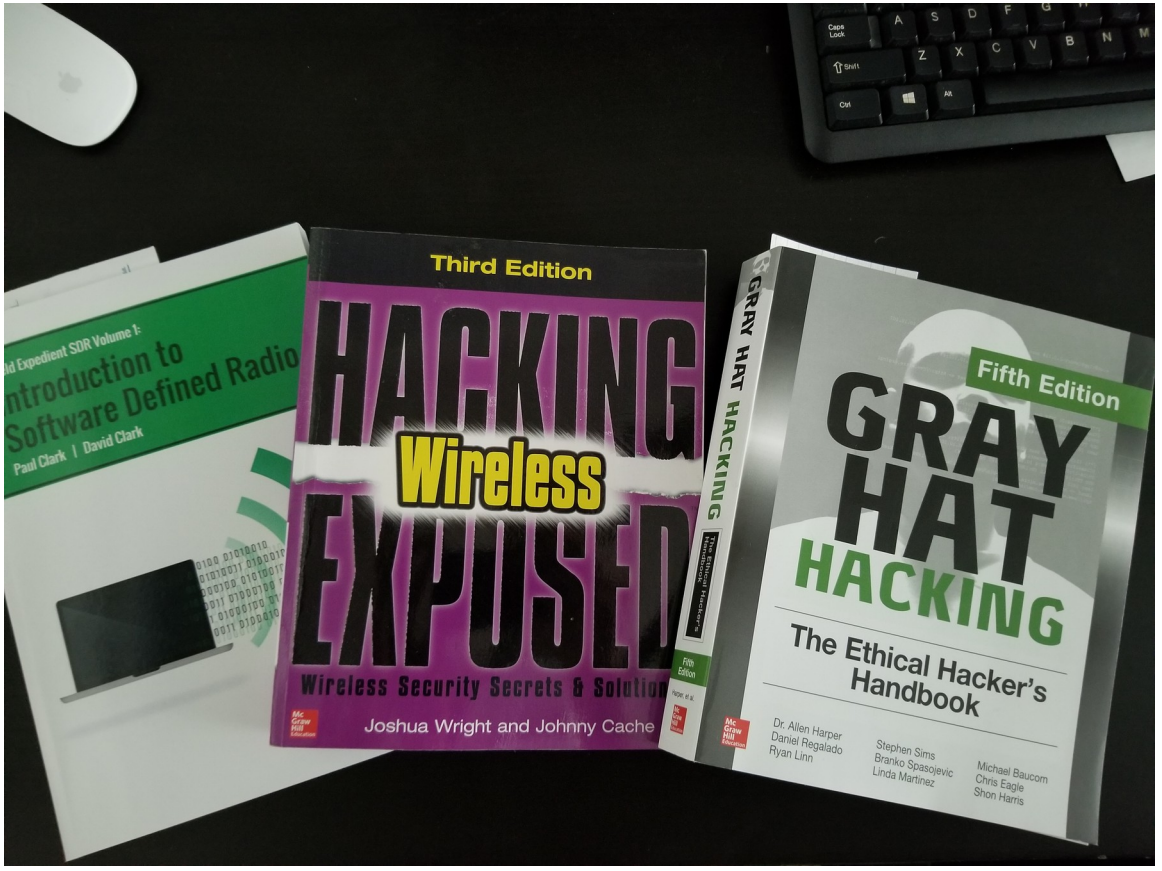
RPITX

- Using Pi Zero to transmit FLEX/POCSAG.
- https://github.com/F5OEO/rpitx

gr-mixalot

- Transmit POCSAG with HackRF One.
- Setup on Parrot, Mint and Raspbian is not as straight forward as one would believe, medium post coming soon.
- https://github.com/unsynchronized/gr-mixalot

Books:


Introduction to
Software Defined Radio
Paul Clark | David Clark
Third Edition
HACKING
Wireless
EXPOSED
Wireless Security Secrets & Solutions
Joshua Wright and Johnny Cache
GRAY HAT HACKING
Fifth Edition
GRAY
HAT
HACKING
The Ethical Hacker's
Handbook
Dr. Allen Harper
Daniel Regalado
Ryan Linn
Stephen Sims
Branko Spasojevic
Linda Martinez
Michael Baucom
Chris Eagle
Shon Harris

FIN

- Twitter: @grnbeltwarrior
- GitHub: https://www.github.com/grnbeltwarrior
- Medium: https://medium.com/@grnbeltwarrior
- PCAP_Search on GitHub (powershell)
- PowerShare_Grep on GitHub (powershell)
- Wireless