GNU Radio

THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

Intro & Updates

Ben Hilburn

What is ‘Software Radio’?

Defined by the IEEE P1900.1 Working Group and the WINNF:

A radio in which some or all of the physical layer functions are software-defined.

IEEE

WIRELESS INNOVATION FORUM

SDR FORUM VERSION 2.0 WIRELESSINNOVATION.ORG

What is ‘Software Radio’?

Defined by the IEEE P1900.1 Working Group and the WINNF:

A radio in which some or all of the physical layer functions are software-defined.

Processing is defined by programmed algorithms, not HW.

What is ‘Software Radio’?

Defined by the IEEE P1900.1 Working Group and the WINNF:

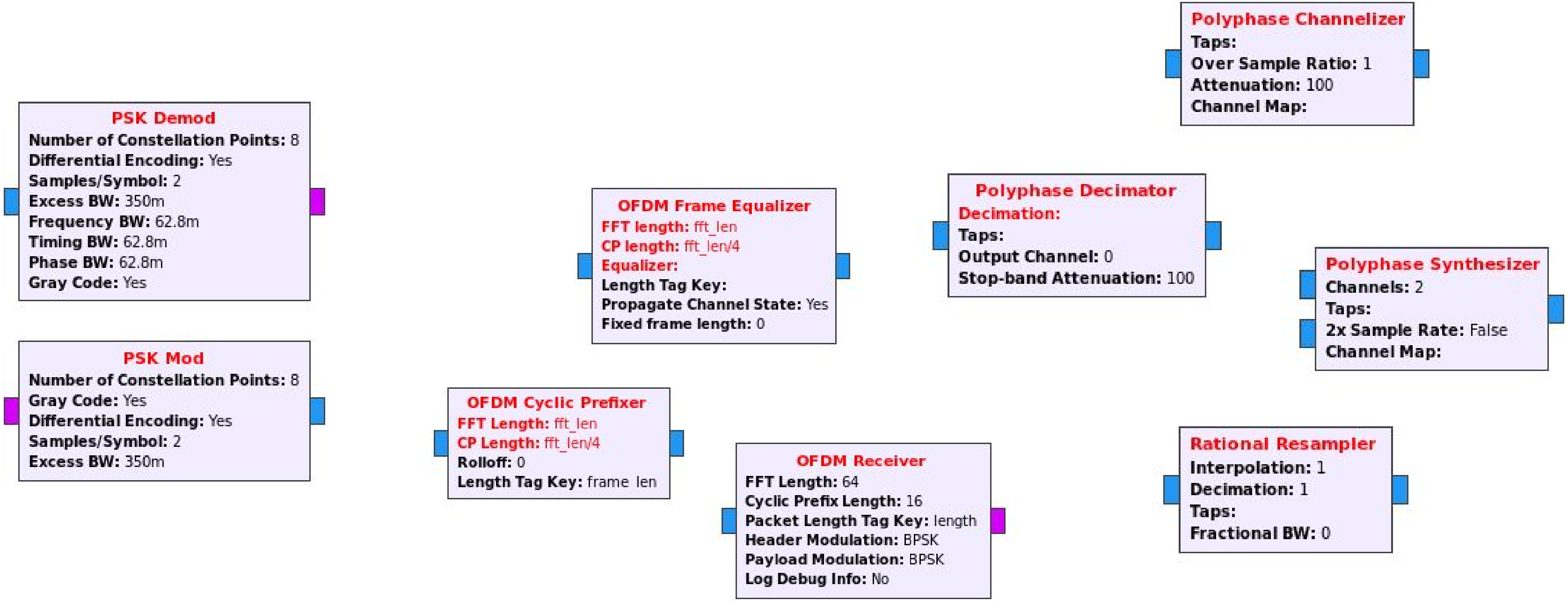
A radio in which some or all of the physical layer functions are software-defined.

Processing is defined by programmed algorithms, not HW.

(‘Software-Defined Radio’ [SDR] is the same thing)

Processing Blocks

- From the, “Okay, that’s useful,” to the “Whoa, that’s awesome.”



Polyphase Channelizer
Taps:
Over Sample Ratio: 1
Attenuation: 100
Channel Map:

PSK Demod
Number of Constellation Points: 8
Differential Encoding: Yes
Samples/Symbol: 2
Excess BW: 350m
Frequency BW: 62.8m
Timing BW: 62.8m
Phase BW: 62.8m
Gray Code: Yes

OFDM Frame Equalizer
FFT length: fft_len
CP length: fft_len/4
Equalizer:
Length Tag Key:
Propagate Channel State: Yes
Fixed frame length: 0

Polyphase Decimator
Decimation:
Taps:
Output Channel: 0
Stop-band Attenuation: 100

Polyphase Synthesizer
Channels: 2
Taps:
2x Sample Rate: False
Channel Map:

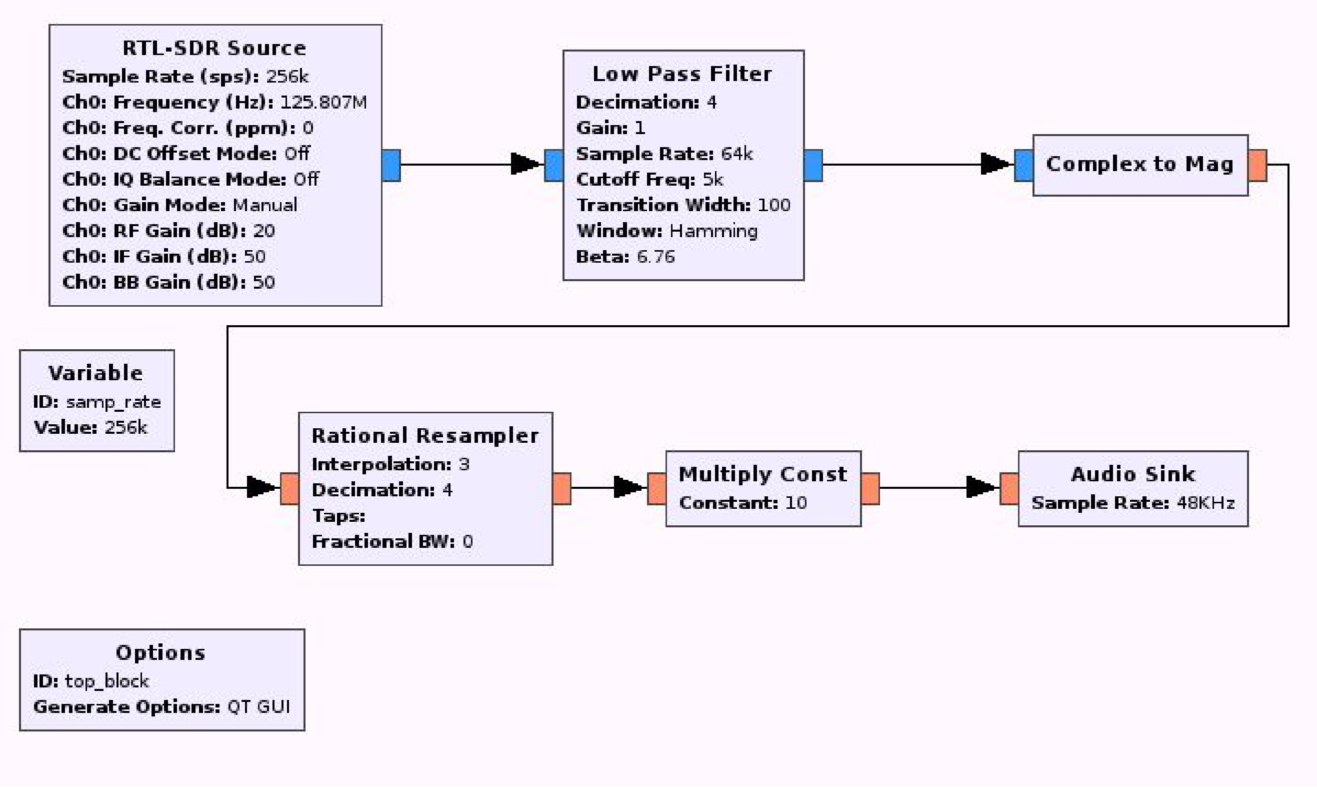
PSK Mod
Number of Constellation Points: 8
Gray Code: Yes
Differential Encoding: Yes
Samples/Symbol: 2
Excess BW: 350m

OFDM Cyclic Prefixer
FFT Length: fft_len
CP Length: fft_len/4
Rolloff: 0
Length Tag Key: frame_len

Rational Resampler
Interpolation: 1
Decimation: 1
Taps:
Fractional BW: 0

OFDM Receiver
FFT Length: 64
Cyclic Prefix Length: 16
Packet Length Tag Key: length
Header Modulation: BPSK
Payload Modulation: BPSK
Log Debug Info: No

Flowgraphs



RTL-SDR Source
Sample Rate (sps): 256k
Ch0: Frequency (Hz): 125.807M
Ch0: Freq. Corr. (ppm): 0
Ch0: DC Offset Mode: Off
Ch0: IQ Balance Mode: Off
Ch0: Gain Mode: Manual
Ch0: RF Gain (dB): 20
Ch0: IF Gain (dB): 50
Ch0: BB Gain (dB): 50

Low Pass Filter
Decimation: 4
Gain: 1
Sample Rate: 64k
Cutoff Freq: 5k
Transition Width: 100
Window: Hamming
Beta: 6.76

Complex to Mag

Variable
ID: samp_rate
Value: 256k

Rational Resampler
Interpolation: 3
Decimation: 4
Taps:
Fractional BW: 0

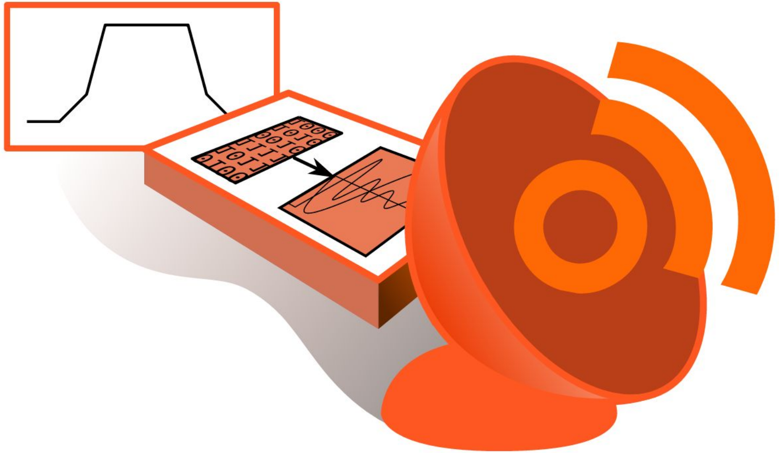
Multiply Const
Constant: 10

Audio Sink
Sample Rate: 48KHz

Options
ID: top_block
Generate Options: QT GUI

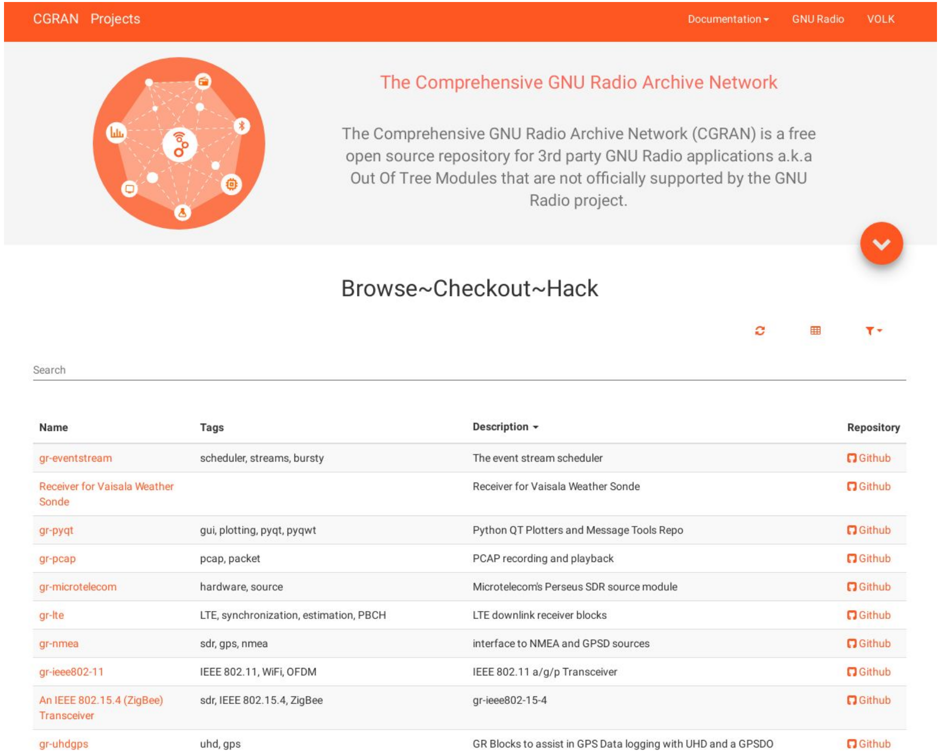
Unified Workflow from Design →Deployment

- Simulate
- Hardware-in-the-Loop Prototyping
- Deploy



GNURadio
THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

Out of Tree Modules



CGRAN Projects

Documentation ▾ GNU Radio VOLK

The Comprehensive GNU Radio Archive Network

The Comprehensive GNU Radio Archive Network (CGRAN) is a free open source repository for 3rd party GNU Radio applications a.k.a Out Of Tree Modules that are not officially supported by the GNU Radio project.

Browse~Checkout~Hack

Search

Name	Tags	Description ▾	Repository
gr-eventstream	scheduler, streams, bursty	The event stream scheduler	Github
Receiver for Vaisala Weather Sonde		Receiver for Vaisala Weather Sonde	Github
gr-pyqt	gui, plotting, pyqt, pyqwt	Python QT Plotters and Message Tools Repo	Github
gr-pcap	pcap, packet	PCAP recording and playback	Github
gr-microtelecom	hardware, source	Microtelecom's Perseus SDR source module	Github
gr-lte	LTE, synchronization, estimation, PBCH	LTE downlink receiver blocks	Github
gr-nmea	sdr, gps, nmea	interface to NMEA and GPSD sources	Github
gr-ieee802-11	IEEE 802.11, WiFi, OFDM	IEEE 802.11 a/g/p Transceiver	Github
An IEEE 802.15.4 (ZigBee) Transceiver	sdr, IEEE 802.15.4, ZigBee	gr-ieee802-15-4	Github
gr-uhdgps	uhd, gps	GR Blocks to assist in GPS Data logging with UHD and a GPSDO	Github

GSoC & SOCIS 2017

- Don’t have to be an RF / DSP / Wireless expert to participate!
- Organized by GNU Radio Community Manager: Martin Braun
- History:
  - Google Summer of Code: 2012, 2013, 2014, 2016
  - Summer of Code in Space: 2015, 2016
- Ideas for 2017:
  - General: C++ Flowgraph Generation from GRC, Android, Qt Graphics
  - DSP: RADAR, DAB, Filter Design Tools
  - Security: Fuzzing, View-Only, Auditing
- Ideas List must be finalized next week!

GNU Radio Conference

- GRCon17 will be our 7th year
  - Finalizing San Diego!
  - Mid-September
- GRCon16:
  - Hosted in Boulder, Colorado
  - 304 Attendees, 20 Sponsors
  - 51+ Tech Talks
  - 4 Days of Talks
  - 1 Day of Hackfest
  - Hacking Challenge

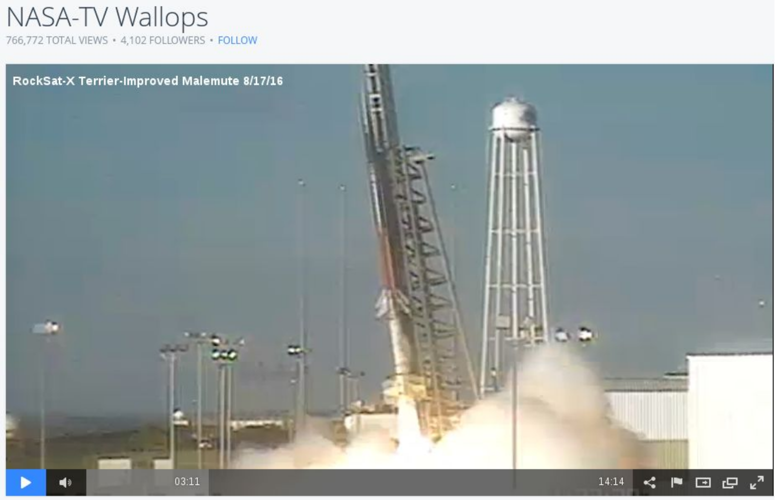
GRCon`16

GNU Radio Foundation (, Inc.)

- Incorporated last year!
- Current responsibilities:
  - Raising money to support the project
  - Managing finances
  - Holding & managing all IP not owned by the FSF
  - Paying for & maintaining our (significant) AWS infrastructure
  - Putting on GRCon
- Future responsibilities:
  - Funding project development

Virginia Tech Ground Station & Sounding Rocket

- GNU Radio in the rocket, GNU Radio on the ground!



NASA-TV Wallops

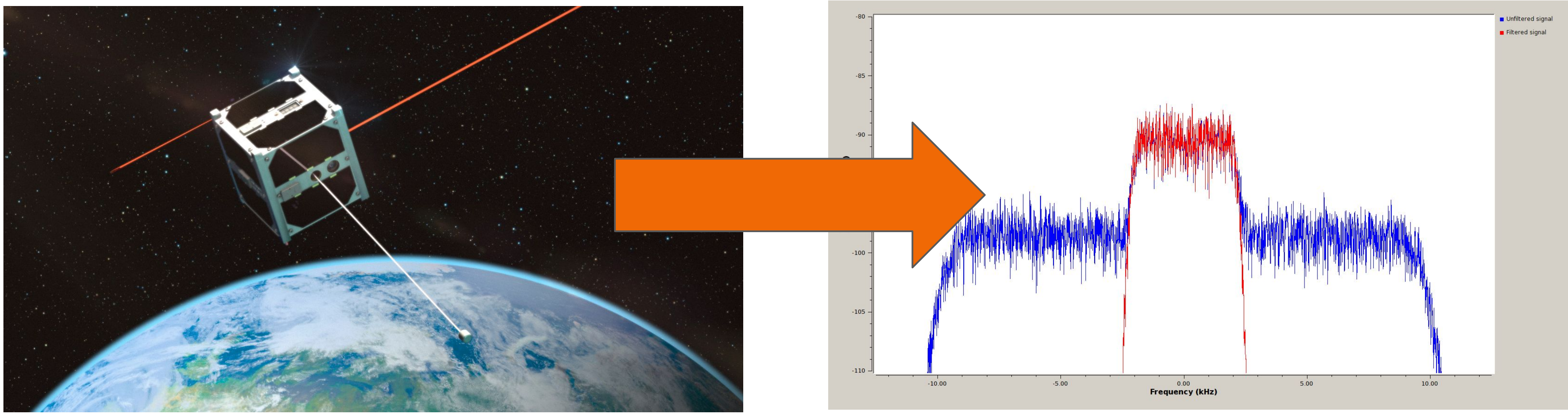
766,772 TOTAL VIEWS • 4,102 FOLLOWERS • FOLLOW

RockSat-X Terrier-Improved Malemute 8/17/16

VirginiaTech
Hume Center for National
Security and Technology

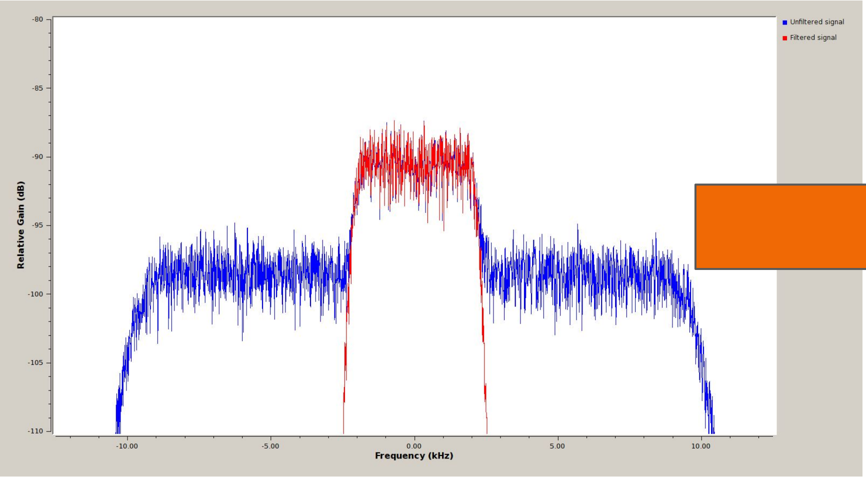
GNURadio
THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

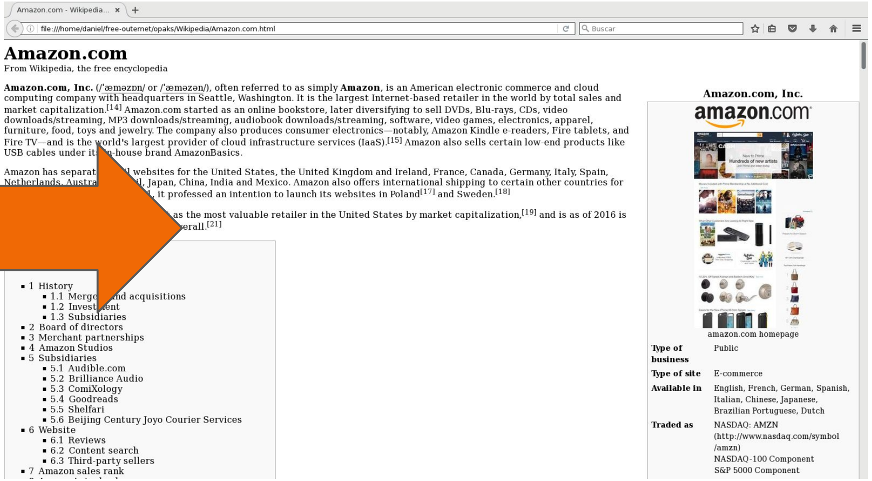
Reverse Engineering Outernet



Blog Post Walkthrough: http://gnuradio.org/blog/reverse-engineering-outernet/

Reverse Engineering Outernet





Amazon.com - Wikipedia...
file:///home/daniel/free-outernet/opaks/Wikipedia/Amazon.com.html
Buscar

Amazon.com

From Wikipedia, the free encyclopedia

Amazon.com, Inc. (/ˈæməzɒn/ or /ˈæməzən/), often referred to as simply **Amazon**, is an American electronic commerce and cloud computing company with headquarters in Seattle, Washington. It is the largest Internet-based retailer in the world by total sales and market capitalization.[14] Amazon.com started as an online bookstore, later diversifying to sell DVDs, Blu-rays, CDs, video downloads/streaming, MP3 downloads/streaming, audiobook downloads/streaming, software, video games, electronics, apparel, furniture, food, toys and jewelry. The company also produces consumer electronics—notably, Amazon Kindle e-readers, Fire tablets, and Fire TV—and is the world's largest provider of cloud infrastructure services (IaaS).[15] Amazon also sells certain low-end products like USB cables under its in-house brand AmazonBasics.

Amazon has separat [illegible] l websites for the United States, the United Kingdom and Ireland, France, Canada, Germany, Italy, Spain, Netherlands, Austra [illegible] il, Japan, China, India and Mexico. Amazon also offers international shipping to certain other countries for [illegible] 1, it professed an intention to launch its websites in Poland[17] and Sweden.[18]

[illegible] as the most valuable retailer in the United States by market capitalization,[19] and is as of 2016 is [illegible] erall.[21]

- 1 History
  - 1.1 Merge[illegible]nd acquisitions
  - 1.2 Invest[illegible]ent
  - 1.3 Subsidiaries
- 2 Board of directors
- 3 Merchant partnerships
- 4 Amazon Studios
- 5 Subsidiaries
  - 5.1 Audible.com
  - 5.2 Brilliance Audio
  - 5.3 ComiXology
  - 5.4 Goodreads
  - 5.5 Shelfari
  - 5.6 Beijing Century Joyo Courier Services
- 6 Website
  - 6.1 Reviews
  - 6.2 Content search
  - 6.3 Third-party sellers
- 7 Amazon sales rank

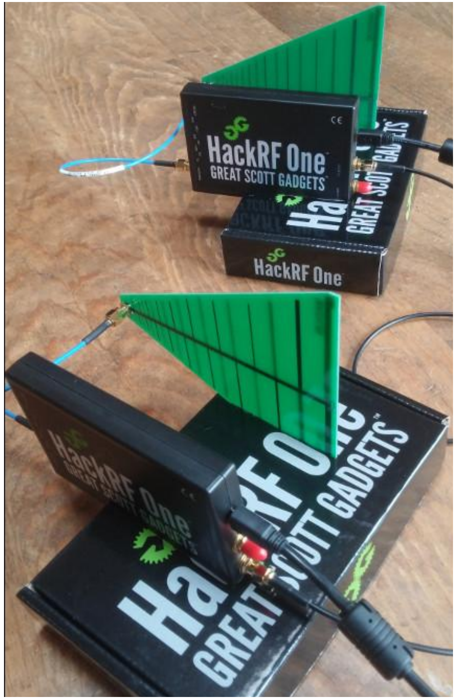
Amazon.com, Inc.

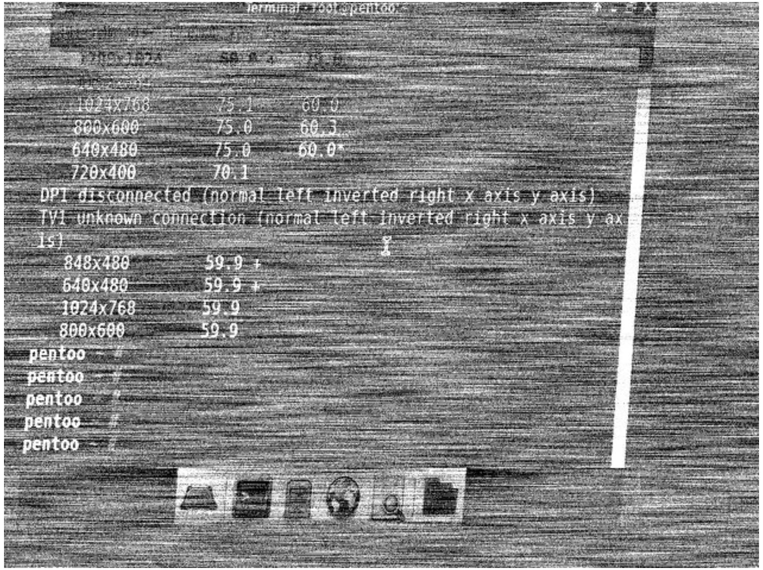
amazon.com homepage

Type of business	Public
Type of site	E-commerce
Available in	English, French, German, Spanish, Italian, Chinese, Japanese, Brazilian Portuguese, Dutch
Traded as	NASDAQ: AMZN (http://www.nasdaq.com/symbol/amzn) NASDAQ-100 Component S&P 5000 Component

Blog Post Walkthrough: http://gnuradio.org/blog/reverse-engineering-outernet/

Sniffing VGA Signals





```
   1280x1024      60.0 +   75.0
   1024x768       75.1     60.0
   800x600        75.0     60.3
   640x480        75.0     60.0*
   720x400        70.1
DPI disconnected (normal left inverted right x axis y axis)
TV1 unknown connection (normal left inverted right x axis y ax
is)
   848x480        59.9 +
   640x480        59.9 +
   1024x768       59.9
   800x600        59.9
pentoo ~ #
pentoo ~ #
pentoo ~ #
pentoo ~ #
pentoo ~ #
```

First presented at GRCon14: Presentation Slides

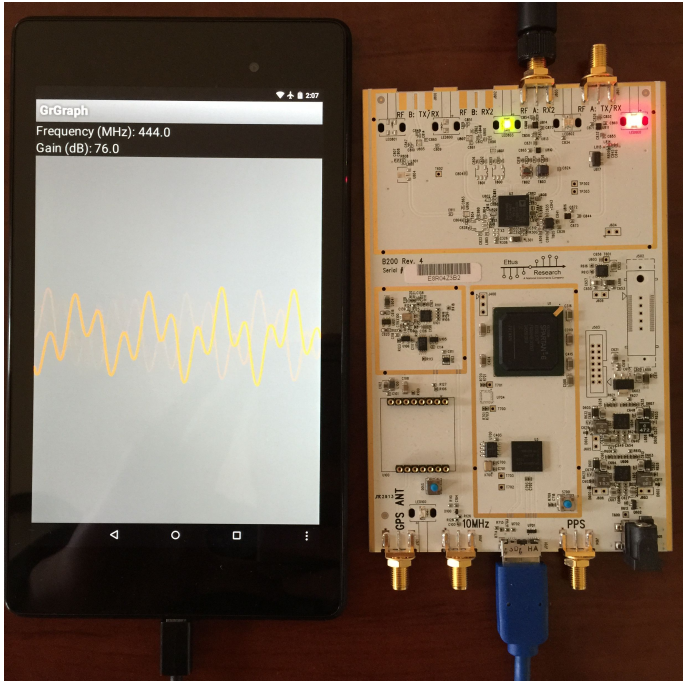
DEF CON 22 - Michael Ossmann - The NSA Playset: RF Retroreflectors

Resurrecting AMPS

- Schmoocon 2017: Dig Out Your Brick Phone! Bringing AMPS Back with GNU Radio
- gr-amps OOT: https://github.com/unsynchronized/gr-amps

Android!

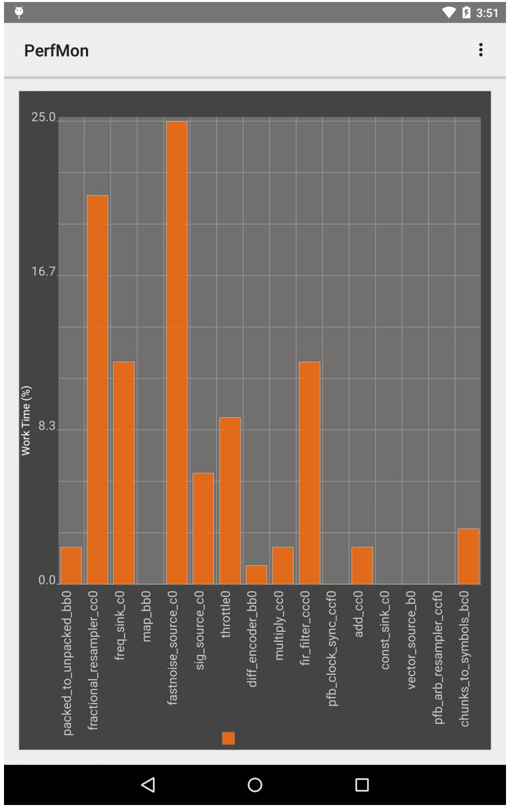
- Original work all done by Tom Rondeau



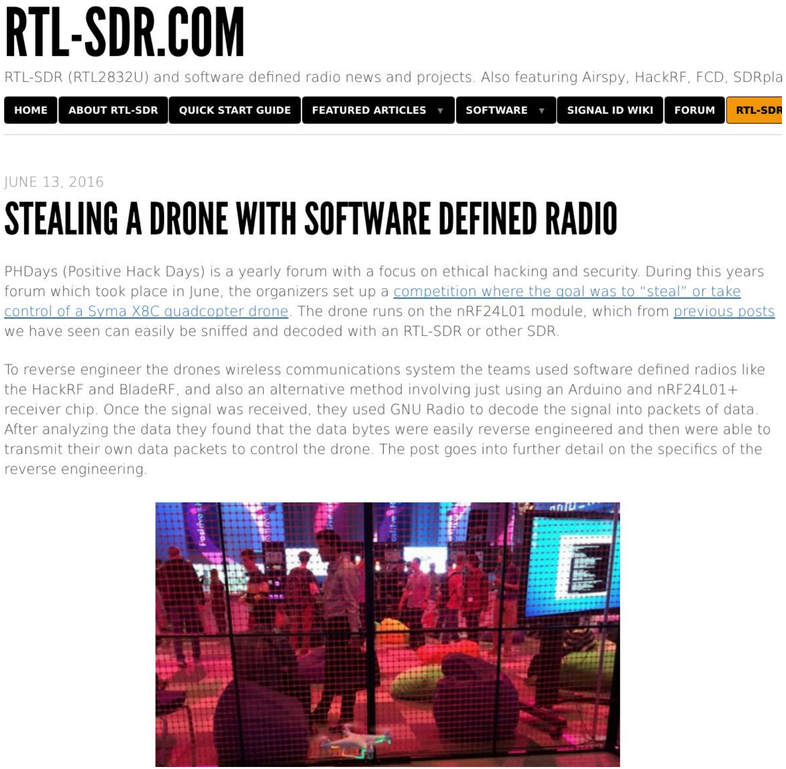
GrGraph

Frequency (MHz): 444.0

Gain (dB): 76.0



Drone Hijacking



RTL-SDR.COM

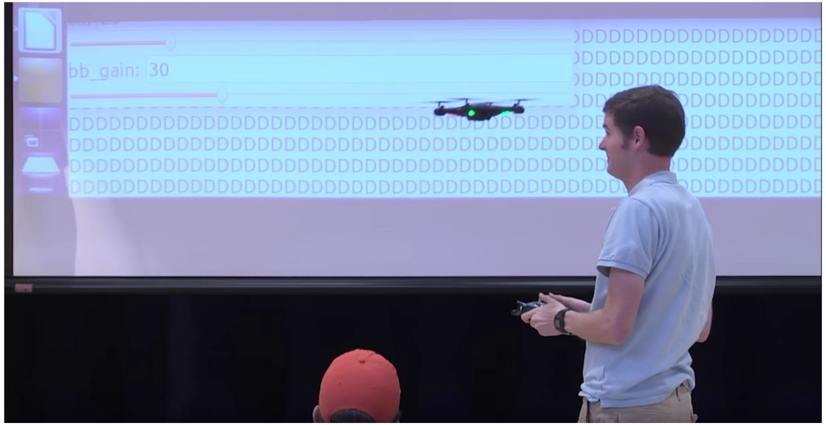
RTL-SDR (RTL2832U) and software defined radio news and projects. Also featuring Airspy, HackRF, FCD, SDRpla

JUNE 13, 2016

STEALING A DRONE WITH SOFTWARE DEFINED RADIO

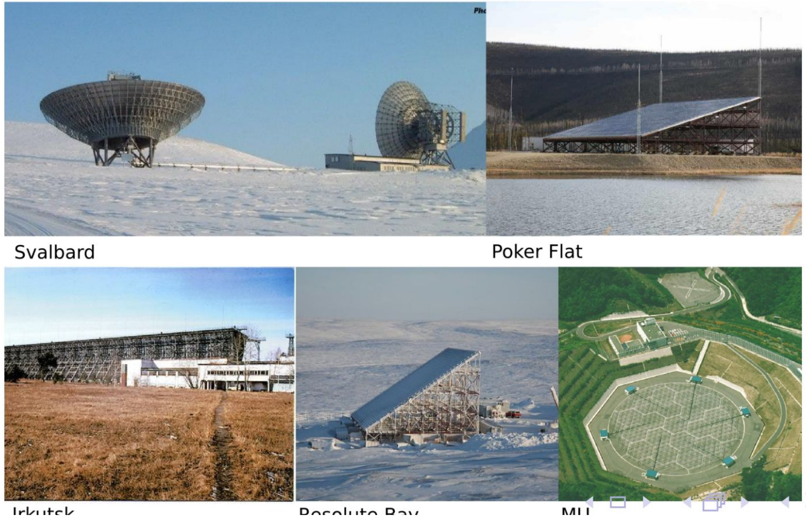
PHDays (Positive Hack Days) is a yearly forum with a focus on ethical hacking and security. During this years forum which took place in June, the organizers set up a competition where the goal was to "steal" or take control of a Syma X8C quadcopter drone. The drone runs on the nRF24L01 module, which from previous posts we have seen can easily be sniffed and decoded with an RTL-SDR or other SDR.

To reverse engineer the drones wireless communications system the teams used software defined radios like the HackRF and BladeRF, and also an alternative method involving just using an Arduino and nRF24L01+ receiver chip. Once the signal was received, they used GNU Radio to decode the signal into packets of data. After analyzing the data they found that the data bytes were easily reverse engineered and then were able to transmit their own data packets to control the drone. The post goes into further detail on the specifics of the reverse engineering.



GRCon16 - Drone Hijacking and Other IoT Hacking, Alexander Chemeris

Radio Astronomy



Images from Juha Vierinen’s presentation:
Geophysical Remote Sensing with GNU Radio

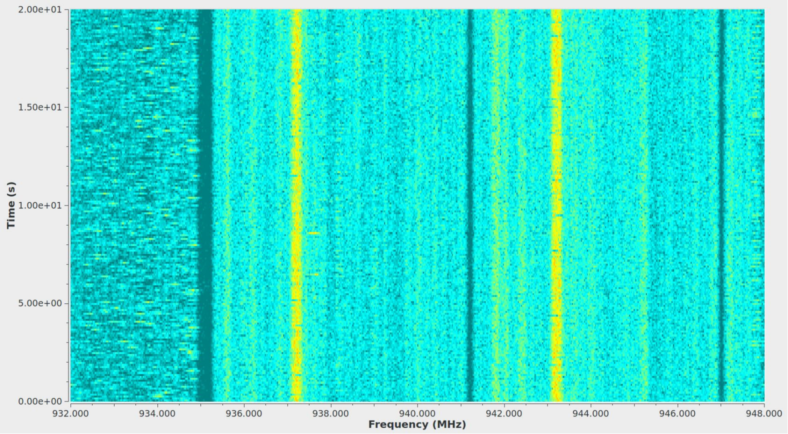
Radio Astronomy

- Juha Vierinen’s work at Haystack Observatory
  - Presented at GRCon13: slides, video
- National Radio Astronomy Observatory
  - Presented at Cyberspectrum 10: Using GNU Radio for Astronomy Research, Public Outreach
- Open Source Radio Telescope Project (OSRT)
  - Building a community for open source radio telescopes
- Canadian Centre for Experimental Radio Astronomy (CCERA)
  - Goal: Make something like this accessible to everyone

GNURadio
THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

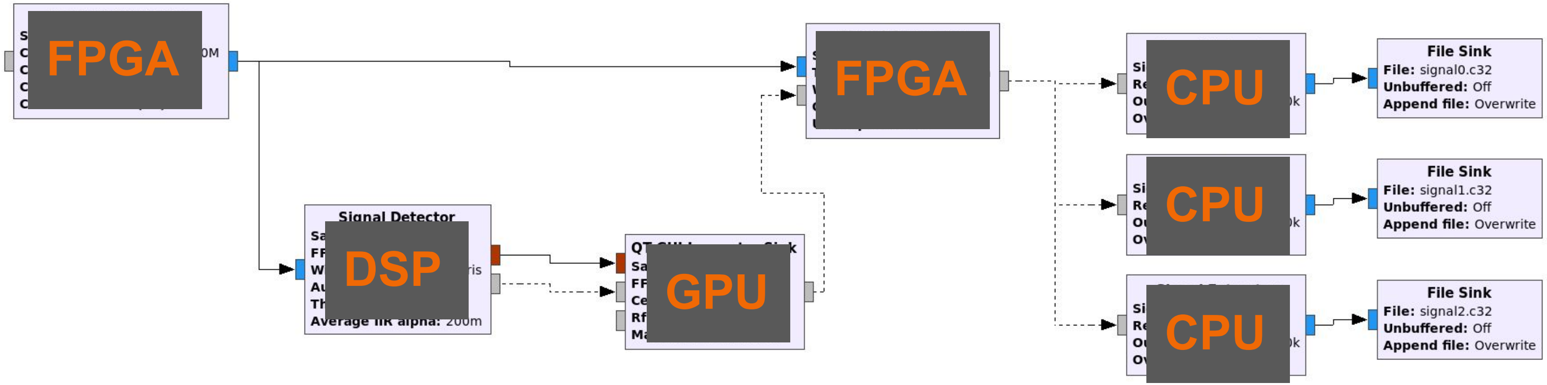
Signal Metadata Format (SigMF)

- Format for describing recordings of digital samples.
- Open Standard
- Why is this useful?
  - Don’t need hardware
  - Signals you don’t have access to
  - Reproducibility (for science!)
  - Collaborative processing
  - Basically “code comments” for signal data
  - Create feature / characteristic annotations
  - Moving data between tools/workflows and retaining meta-information
- Under active development: https://github.com/gnuradio/SigMF



Major Development Directions

- Heterogeneous Processing



Average IIR alpha: 200m

File Sink
File: signal0.c32
Unbuffered: Off
Append file: Overwrite

File Sink
File: signal1.c32
Unbuffered: Off
Append file: Overwrite

File Sink
File: signal2.c32
Unbuffered: Off
Append file: Overwrite

Major Technical Development Directions

- Heterogeneous Processing
- Development Environment
  - Client / Server Architecture
  - Debugging Utilities
  - Qt5 Graphical Tools
- Improvements to GNU Radio ‘core’
  - Memory Management (e.g., more Zero Copy, better NUMA)
  - Parallel Processing
  - Dynamic Flowgraph Reconfiguration
- Performance Optimization

Come Get Involved!

- Huge variety of fields and skill levels.
- Students, Hobbyists, Professionals
- Very welcoming of new developers.

- Conferences, Hackfests, Meetups
- Mailing List, IRC, Dev Calls

CONFERENCE

MEETUP

HACKFEST

DEVELOPERS' CALL

gnuradio.org