Software Defined Radio for Infosec People 101

Garrett Gee

Agenda

- Radio Frequency
- Hardware
- Software
- Decoding (Passive) Examples – Planes, Ships, Pagers
- Hacking (Active) Examples – iOS, Cell Phones, House Alarm System
- Process for Decoding
- Reverse Engineering Example

@ggee - Hacker. Entrepreneur. Autodidact.

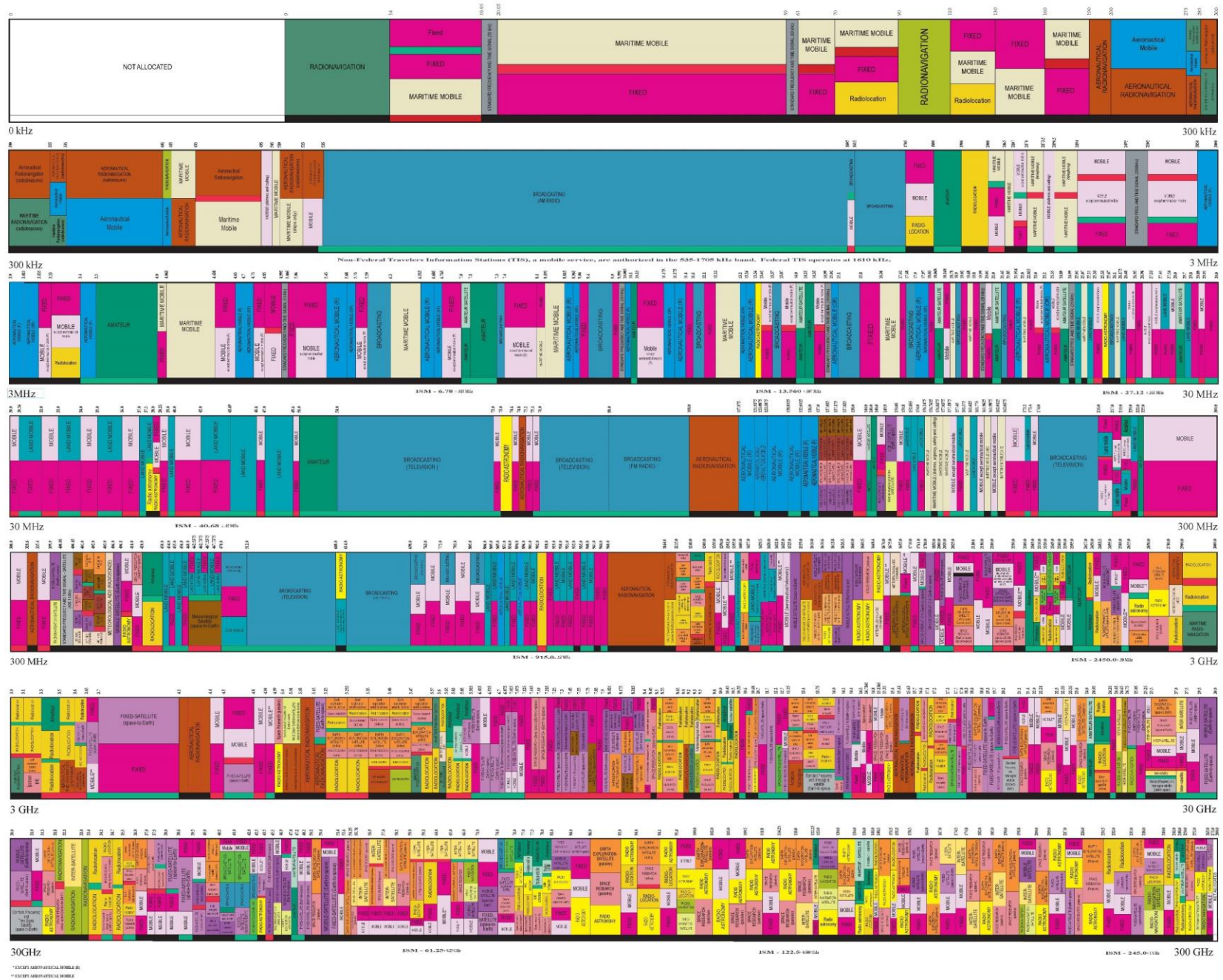
- Hacker
  - 60 Minutes – Cyber War – 2000
  - Portable Linux Auditing CD (PLAC) – 2001
  - Doppelganger Domains – 2011
    - CNN, Wired, The Osgood File, Bloomberg BusinessWeek, BBC
- Entrepreneur
  - Godai Group LLC
  - Hacker Warehouse
  - Infosec Events
- Autodidact

Background – Radio Frequency

- Any electromagnetic wave frequencies that lie in the range extending from around 3 kHz to 300 GHz
- Common Examples
  - AM / FM broadcast radio
  - Cell phones
  - Global Positioning System
  - Pagers
  - Television
  - Wi-Fi

UNITED STATES FREQUENCY ALLOCATIONS

THE RADIO SPECTRUM



Non-Federal Travelers Information Stations (TIS), a mobile service, are authorized in the 535-1705 kHz band. Federal TIS operates at 1610 kHz.

* EXCEPT AERONAUTICAL MOBILE (R)

** EXCEPT AERONAUTICAL MOBILE

RADIO SERVICES COLOR LEGEND

- AERONAUTICAL MOBILE
- AERONAUTICAL MOBILE SATELLITE
- AERONAUTICAL RADIONAVIGATION
- AMATEUR
- AMATEUR SATELLITE
- BROADCASTING
- BROADCASTING SATELLITE
- EARTH EXPLORATION SATELLITE
- FIXED
- FIXED SATELLITE
- INTER-SATELLITE
- LAND MOBILE
- LAND MOBILE SATELLITE
- MARITIME MOBILE
- MARITIME MOBILE SATELLITE
- MARITIME RADIONAVIGATION
- METEOROLOGICAL
- METEOROLOGICAL SATELLITE
- MOBILE
- MOBILE SATELLITE
- RADIO ASTRONOMY
- RADIODETERMINATION SATELLITE
- RADIOLOCATION
- RADIOLOCATION SATELLITE
- RADIONAVIGATION
- RADIONAVIGATION SATELLITE
- SPACE OPERATION
- SPACE RESEARCH
- STANDARD FREQUENCY AND TIME SIGNAL
- STANDARD FREQUENCY AND TIME SIGNAL SATELLITE

ACTIVITY CODE

- FEDERAL EXCLUSIVE
- FEDERAL/NON-FEDERAL SHARED
- NON-FEDERAL EXCLUSIVE

ALLOCATION USAGE DESIGNATION

SERVICE	EXAMPLE	DESCRIPTION
Primary	FIXED	Capital Letters
Secondary	Mobile	1st Capital with lower case letters

This chart is a graphic single-point-in-time portrayal of the Table of Frequency Allocations used by the FCC and NTIA. As such, it may not completely reflect all aspects, i.e. footnotes and recent changes made to the Table of Frequency Allocations. Therefore, for complete information, users should consult the Table to determine the current status of U.S. allocations.

U.S. DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Office of Spectrum Management

JANUARY 2016

PLEASE NOTE: THIS DIAGRAM IS OFFERED FOR SERVICE IN INTERPRETING TREATY STATUTES, AND DOES NOT PURPORT TO BE PROPORTIONAL TO THE ACTUAL AMOUNT OF SPECTRUM ALLOCATED.

Background – Software Defined Radio

- Radio front end
- No dedicated IC backend for decoding radio signal
- Digitize signal and pass it to host system
- Mixers, filters, amplifiers, modulators/demodulators, etc. are all in software
- If you can tune it, you can be that type of radio (in theory)

SDR for Infosec?

- One device can talk to nearly infinite protocols
- Investigate protocols for which there are no public specs or chips
- Investigate protocols for which debugging equipment is $$$, requires you to be a large company, requires NDA, etc.

Hardware

- Lots of SDR devices out there

- Frequency Range
- Bandwidth
- Receive Only / Half Duplex / Full Duplex
- Price

Hardware – RTL-SDR

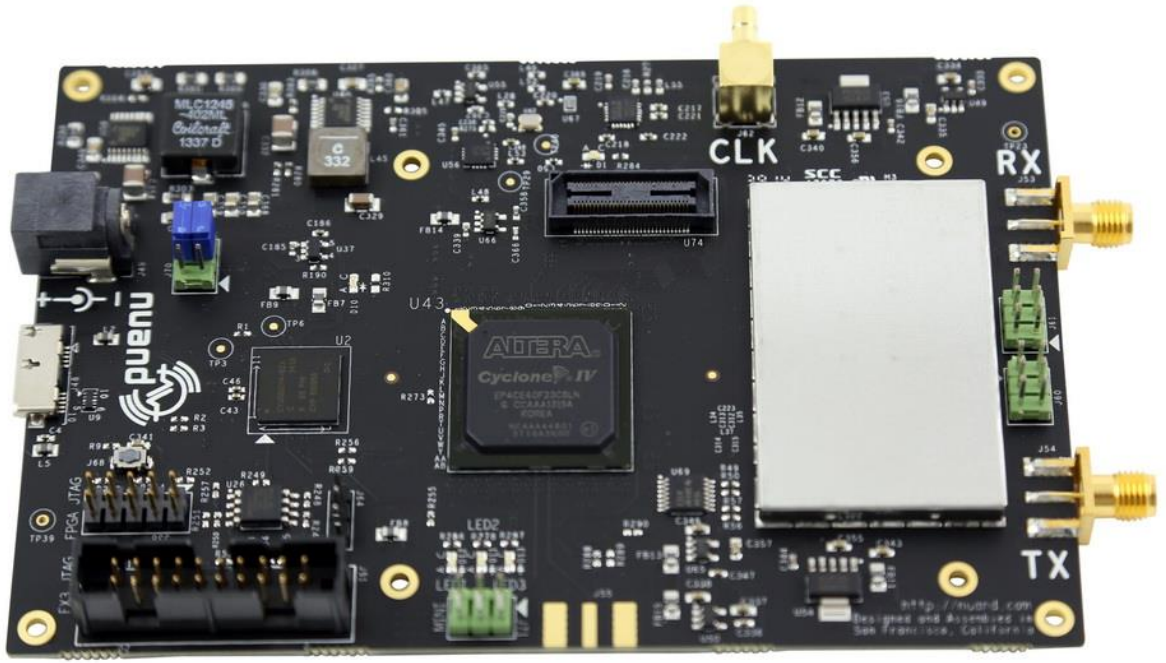
- aka Digital Video Broadcasting – Terrestrial (DVB-T)
- Realtek RTL2832U/R820T Tuner Receiver
- Frequency Range: 24 MHz to 1.8 GHz
- Bandwidth: 2-3 MHz
- Receive only
- ~ $10-$20

Hardware – HackRF One

- Frequency Range: 1 MHz to 6 GHz
- Bandwidth: 20 MHz
- Transmit or receive. Half-duplex
- ~ $330

Hardware – BladeRF x40

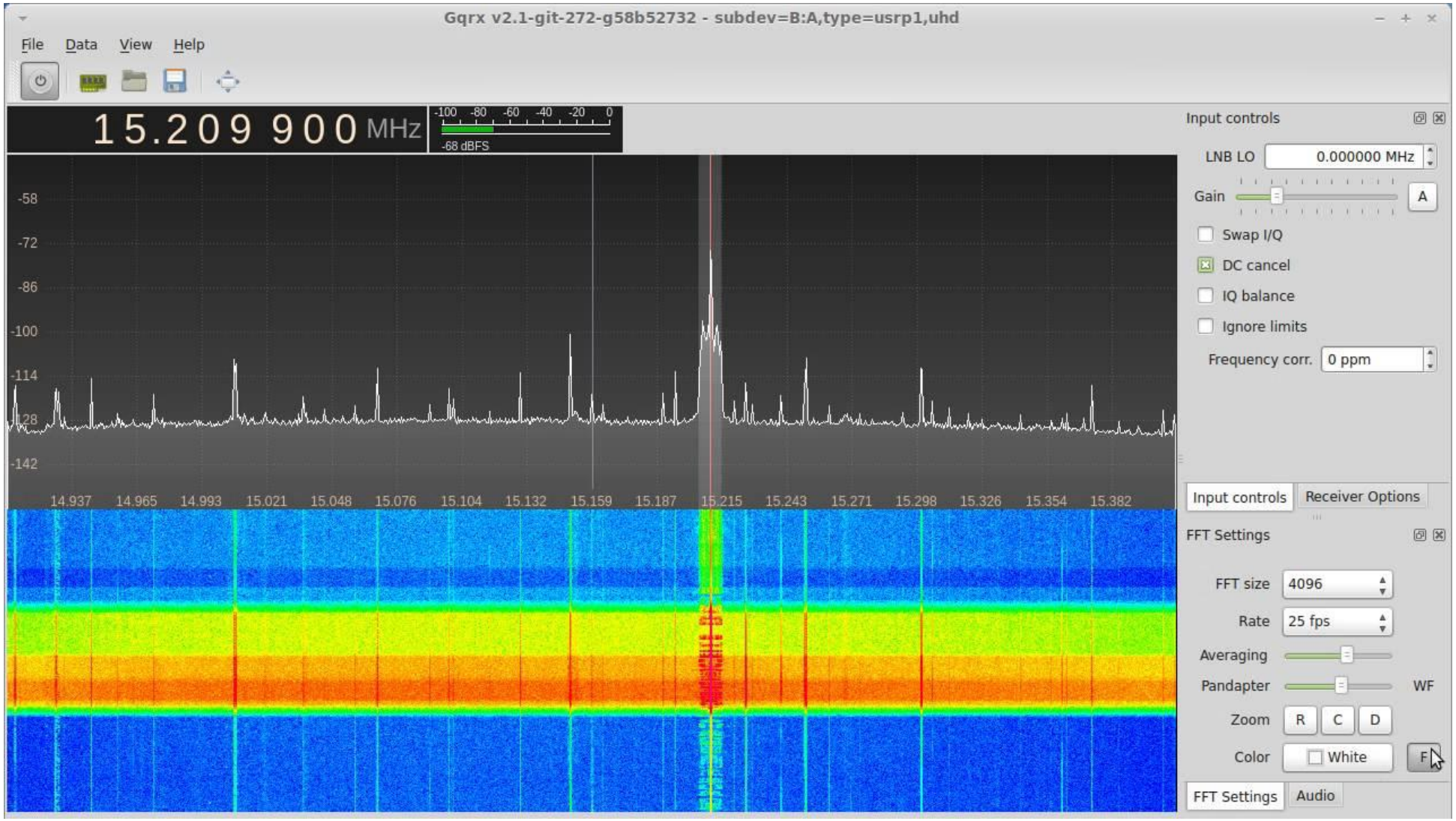
- Frequency Range: 300 MHz to 3.8 GHz
- Bandwidth: 28 MHz
- Transmit and receive. Full-duplex
- ~ $440



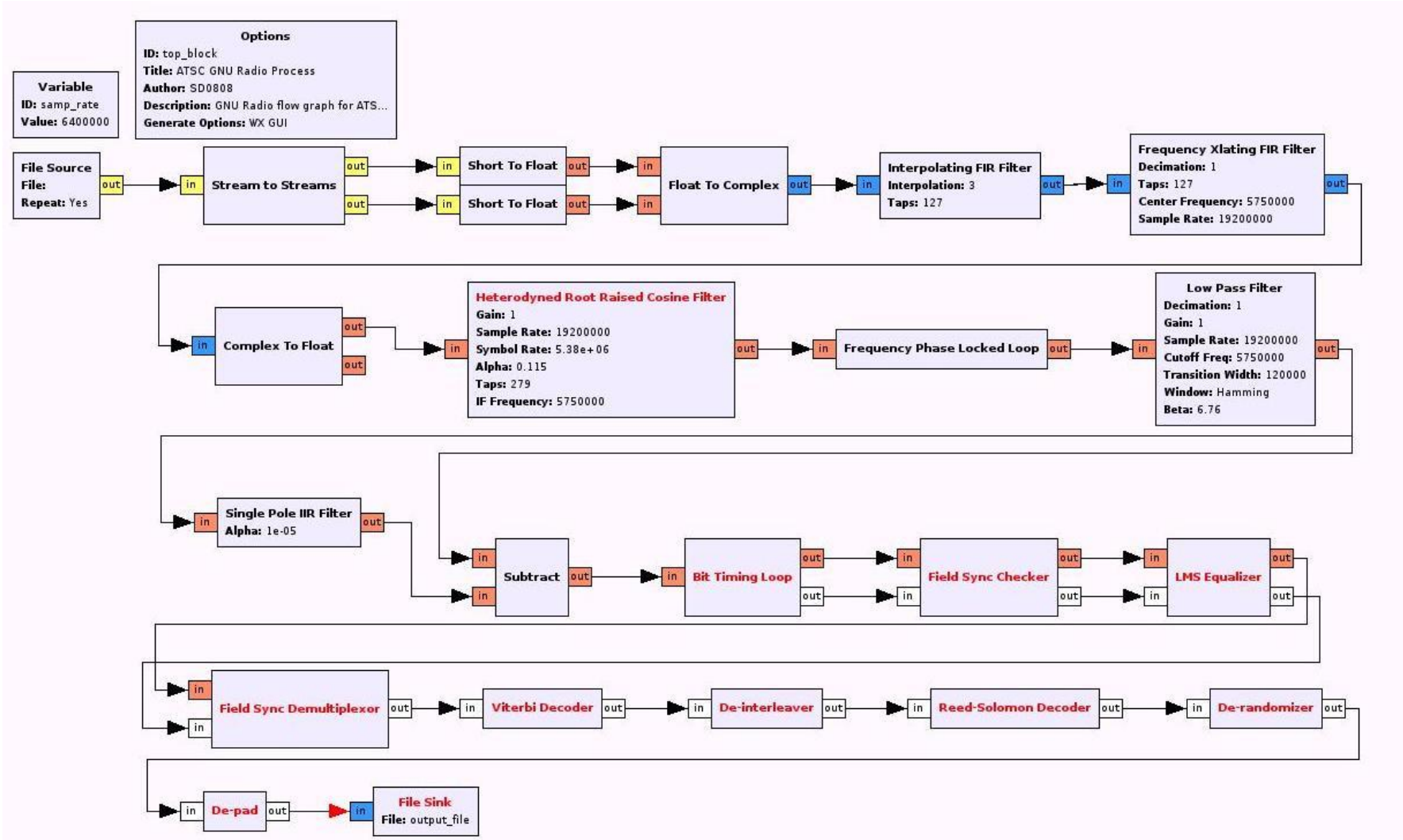
Hardware – USRP

- Several product lines. Bus, Network, X
- Network and X lines have modular RF Daughterboard design
  - UBX board: 10 MHz to 6 GHz, 160 Mhz bandwidth, full-duplex
- ~ $2000-$5000

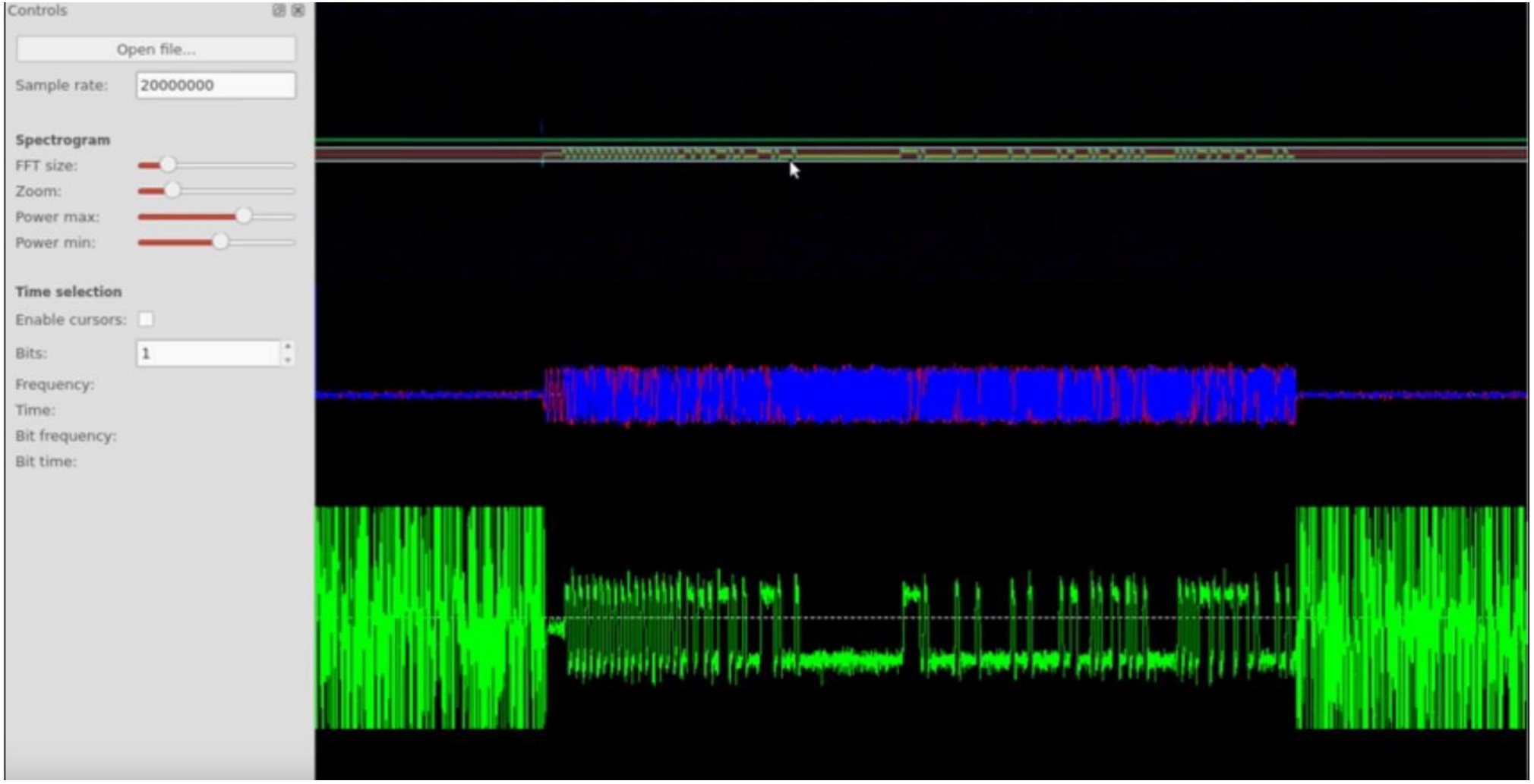
Software – Visualization - GQRX / SDR#



Software – GNU Radio



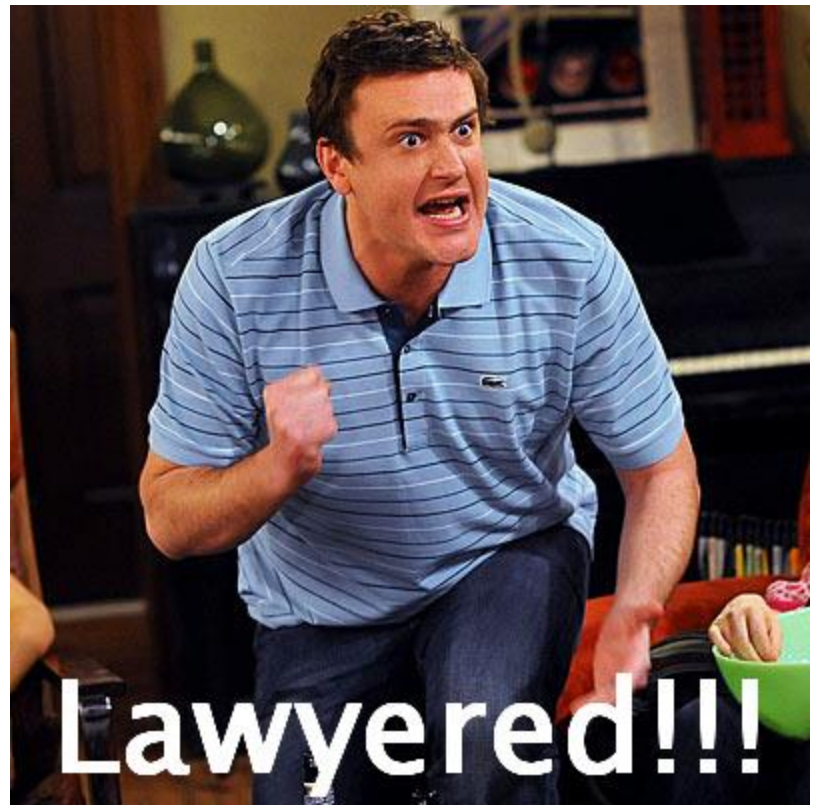
Software - Inspectrum



Software - Python

- GNU Radio
- Matlibplot
- numpy


HACK
ALL THE THINGS
memegenerator.net


Lawyered!!!

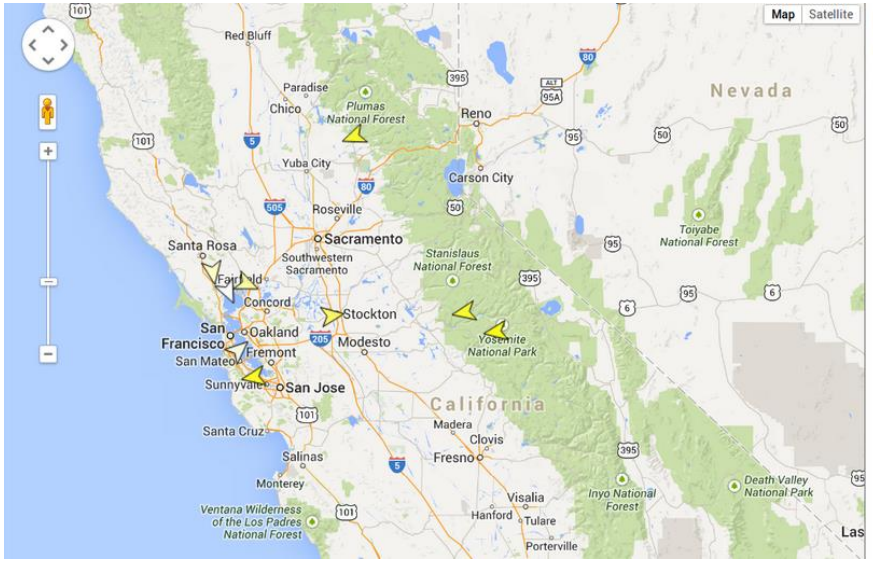
Decoding Example - Planes

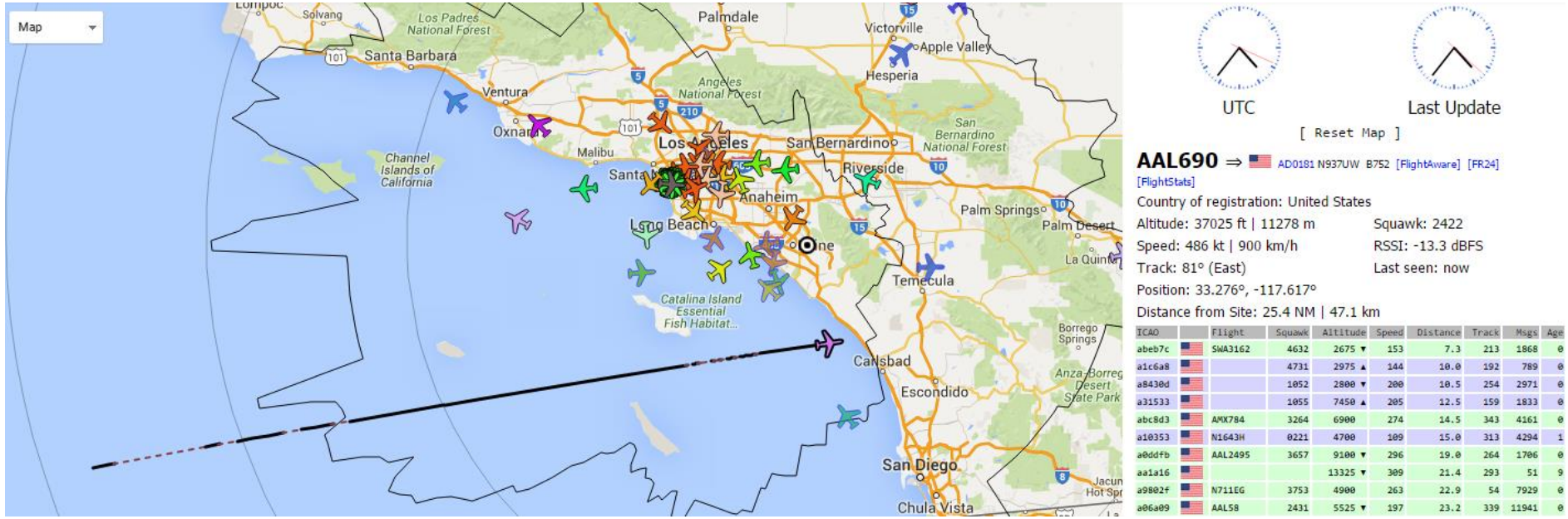
- ADS-B: Automatic Dependent Surveillance – Broadcast
- Aircraft gets position from satellite and broadcasts it for tracking
- No encryption or authentication
- Frequency: 1090 MHz / 978 MHz

Decoding Example – Planes – dump1090

Hex	Mode	Sqwk	Flight	Alt	Spd	Hdg	Lat	Long	Sig	Msgs	Ti-
400e14	S	7315	EZY43PT	37000	419	353			5	42	0
406099	S	7634	CFE59G	38000					5	17	2
484cb6	S	6264	KLM65G	36325	413	297	55.844	-0.518	5	88	0
406a2e	S	7615	GMA104T	28000					4	100	2
400fba	S	5431	BEE1VB	5350					35	733	0
4ca281	S	7322	VIR3007	33175	396	336	54.564	-2.611	12	946	0
400ad1	S	7607		20025					7	208	0
400721	S	4246	LOG47LU	8550					30	955	0
400c5c	S	1444		27025					5	95	32
40610e	S	7330	BEE3FU	24000					9	583	0
400cb9	S	7732	LOG79ES	14500					11	922	0
4012d2	S	5466	LOG34YT	7100					6	83	5
405633	S	6254	EZY44NH	19425	387	149	55.408	-4.174	6	3039	13
400617	S	3416	TCX61EF	21550	439	108	55.364	-3.253	16	5062	0
405f79	S	4477	BEE767	19125					38	6845	0
400984	S	4622	EZE28Z	21475					12	3243	0
4ca73d	S	4244	RYR6699	3250	156	279	56.017	-3.135	81	6853	0
400987	S	4621	EZE76LK	23475					11	6841	0
400691	S	7762	BAW9CG	32675	458	317	56.386	-4.997	11	16051	0
4066d1	S	2227	TOM296	33225	488	151	54.700	-3.405	8	8244	0
4008fb	S	7655	LOG74HR	17600					10	5627	0
491304	S	7646	CSDXD	40000					8	5268	0

Decoding Example – Planes – dump1090





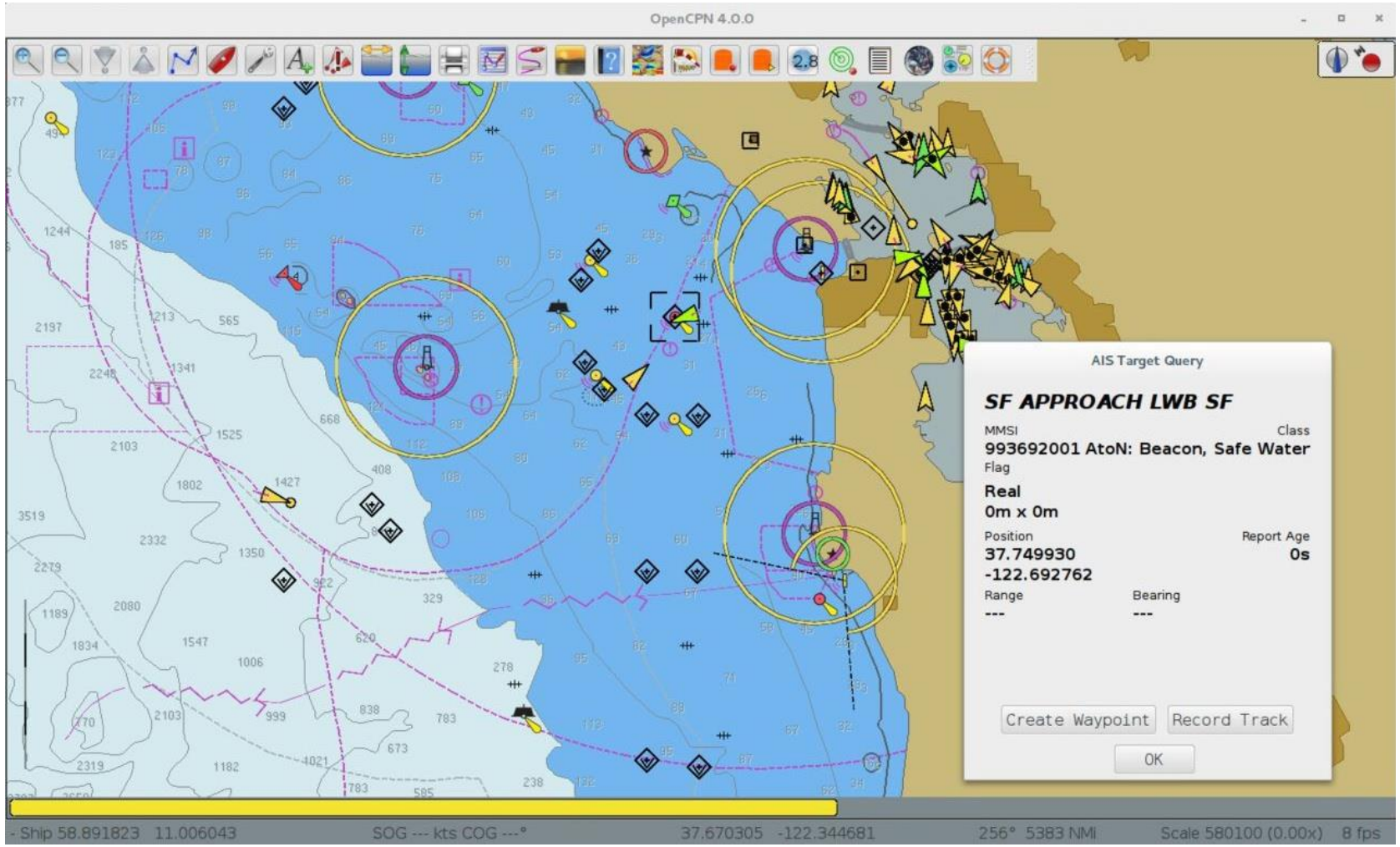
ICAO		Flight	Squawk	Altitude	Speed	Distance	Track	Msgs	Age
abeb7c		SWA3162	4632	2675 ▼	153	7.3	213	1868	0
a1c6a8			4731	2975 ▲	144	10.0	192	789	0
a8430d			1052	2800 ▼	200	10.5	254	2971	0
a31533			1055	7450 ▲	205	12.5	159	1833	0
abc8d3		AMX784	3264	6900	274	14.5	343	4161	0
a10353		N1643H	0221	4700	109	15.0	313	4294	1
a0ddfb		AAL2495	3657	9100 ▼	296	19.0	264	1706	0
aa1a16				13325 ▼	309	21.4	293	51	9
a9802f		N711EG	3753	4900	263	22.9	54	7929	0
a06a09		AAL58	2431	5525 ▼	197	23.2	339	11941	0

Decoding Example - Ships

- AIS: Automatic Identification System
- Similar protocol to ADS-B
- Frequency: 162 MHz

Decoding Example – Ships – gr-ais / opencpn

- gr-ais for receiving data
- Opencpn to map



Decoding Example - Pagers

- POCSAG: Post Office Code Standardization Advisory Group
- Frequencies: 35.22 / 35.58 / 43.22 / 43.58 / 152.0075 (medical) / 152.2700 / 152.4800 / 157.4500 (medical) / 158.1000 / 158.7000 / 163.2500 (medical) / 454.0125 - 454.5000 / 462.7500 – 462.9250 / 465.0000 / 929.0125 – 929.9875 / 931.0125 – 931.9875
- Gqrx | multimon-ng

Hacking (Active) Examples and Thoughts

ANDY GREENBERG SECURITY 06.04.15 7:00 AM

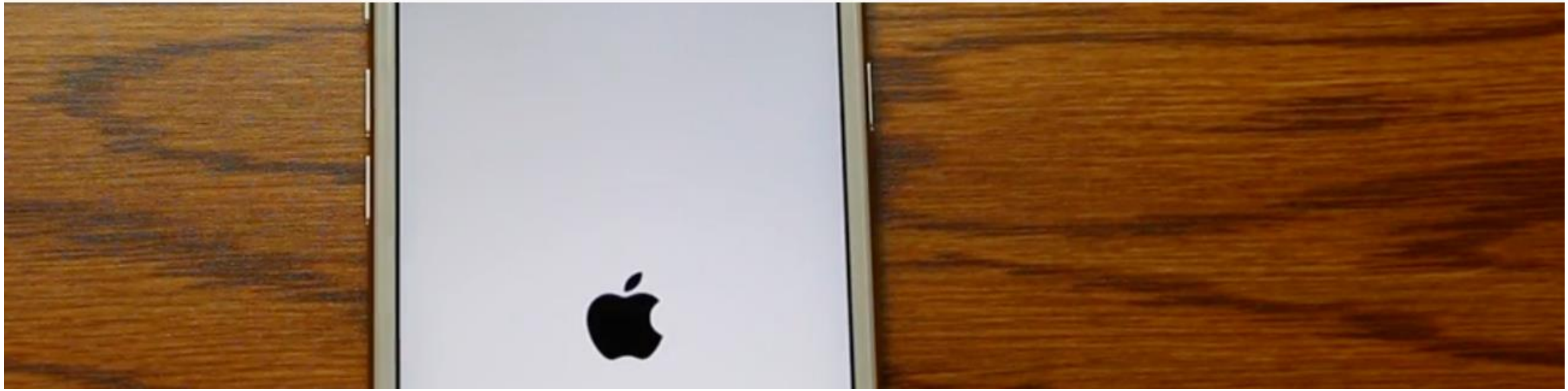
THIS HACKED KIDS' TOY OPENS GARAGE DOORS IN SECONDS

GETTY IMAGES

Apple officially acknowledges iPhone bricking '1970 date' bug, says upcoming software update will fix

Benjamin Mayo - 2 months ago @bzamayo

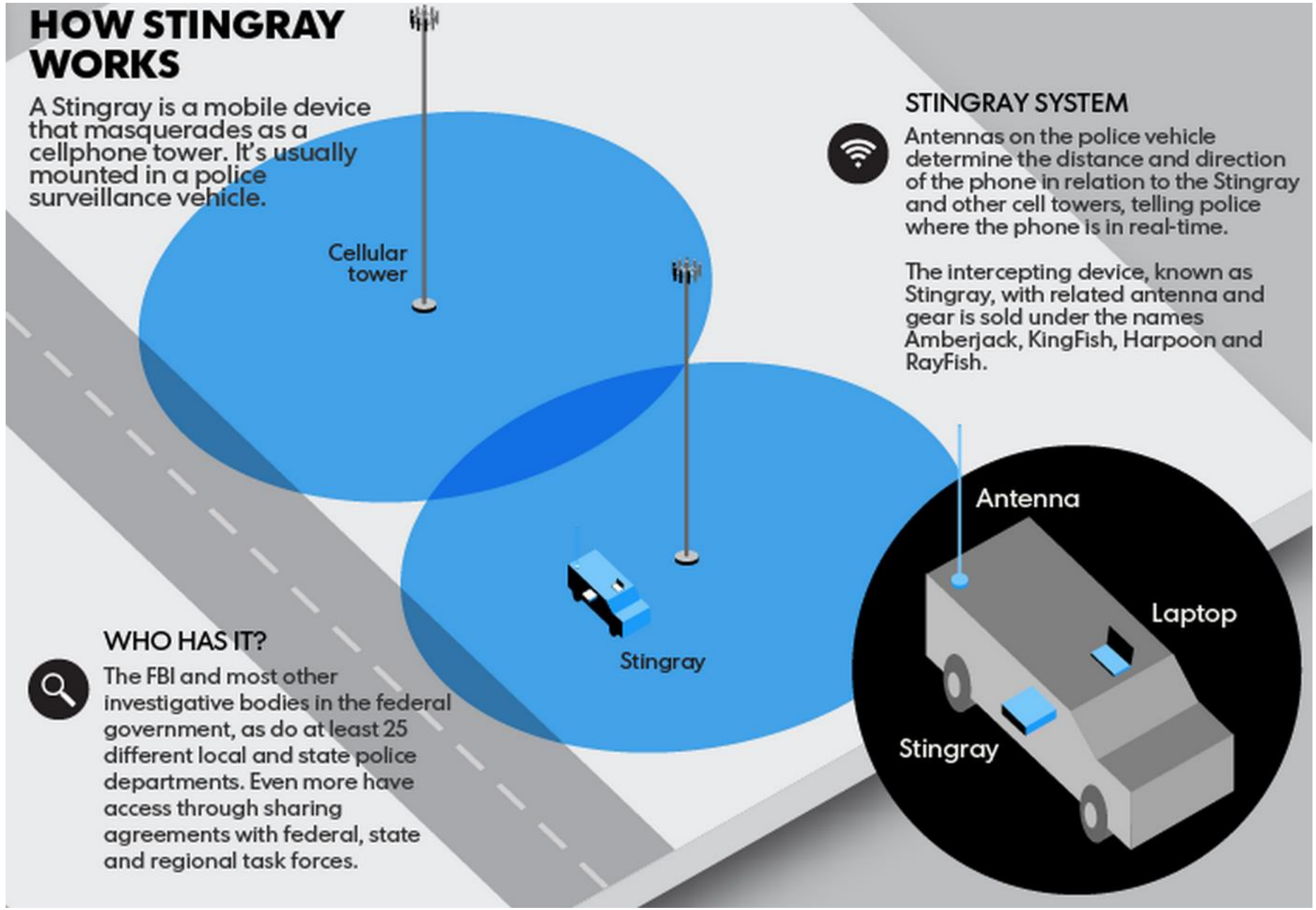
AAPL COMPANY IOS IOS DEVICES



HACK DISARMS SIMPLISAFE'S HOME WIRELESS SECURITY SYSTEMS

by Tom Spring

February 18, 2016 , 4:54 pm


HOW STINGRAY WORKS
A Stingray is a mobile device that masquerades as a cellphone tower. It's usually mounted in a police surveillance vehicle.
Cellular tower
Stingray
STINGRAY SYSTEM
Antennas on the police vehicle determine the distance and direction of the phone in relation to the Stingray and other cell towers, telling police where the phone is in real-time.
The intercepting device, known as Stingray, with related antenna and gear is sold under the names Amberjack, KingFish, Harpoon and RayFish.
Antenna
Laptop
Stingray
WHO HAS IT?
The FBI and most other investigative bodies in the federal government, as do at least 25 different local and state police departments. Even more have access through sharing agreements with federal, state and regional task forces.

ANDY GREENBERG SECURITY 03.21.16 10:33 AM

RADIO ATTACK LETS HACKERS STEAL 24 DIFFERENT CAR MODELS

Other Interesting Systems

- Smart Meters
- Door Access Systems (ex. HID)
- Toll Tags (ex. FasTrak)
- Touch Payment Systems

Process for Decoding - 3 steps

- Determine Frequency
- Determine Modulation
- Determine Protocol / Structure

Restaurant Pagers from Long Range Systems

1 - Determine Frequency

- FCC database
  - https://www.fcc.gov/general/fcc-id-search-page
  - https://fcc.io/

1 results were found that match the search criteria:
Grantee Code: M74 Product Code: T7400

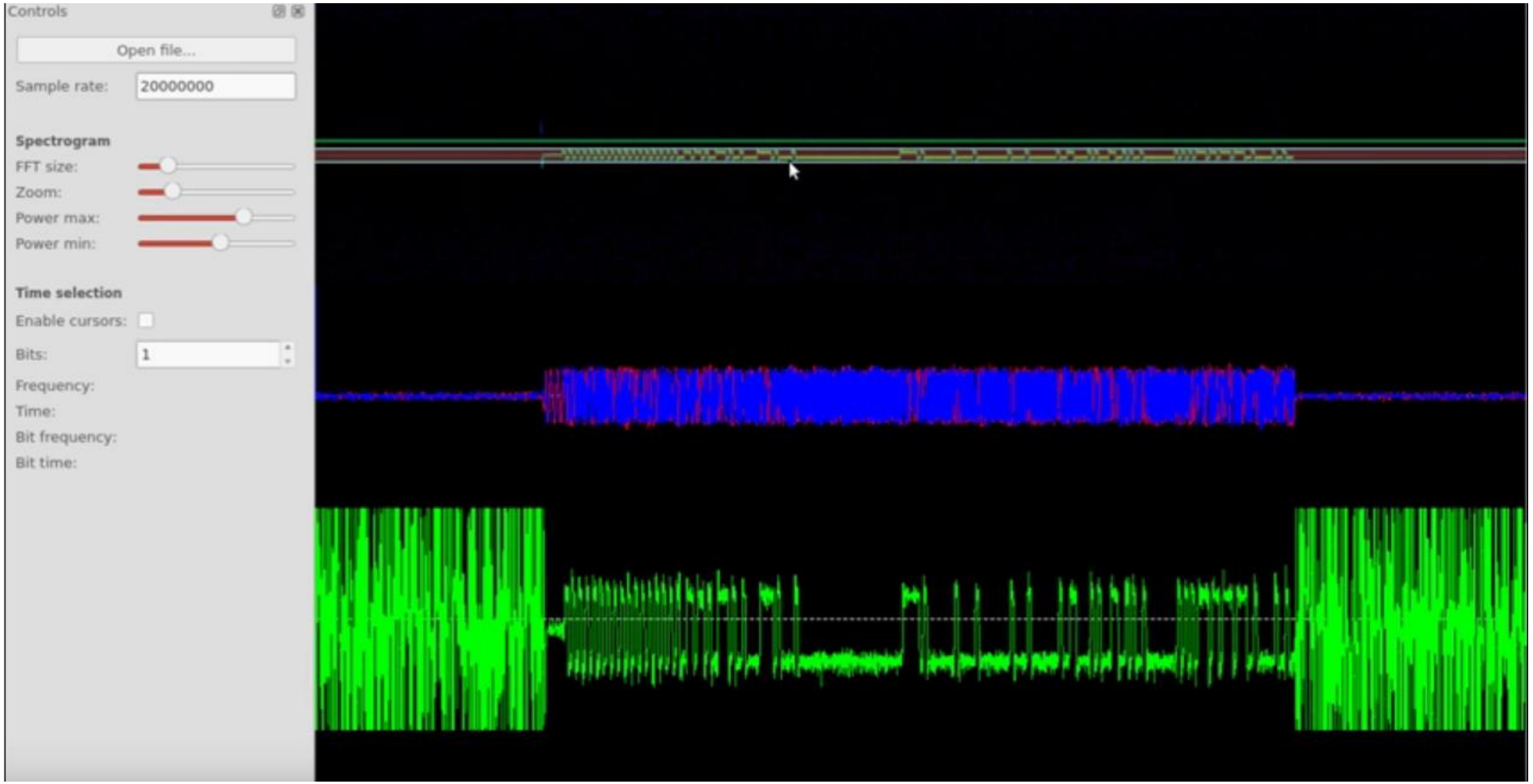
Displaying records 1 through 1 of 1.

View Form	Display Exhibits	Display Grant	Display Correspondence	Applicant Name	Address	City	State	Country	Zip Code	FCC ID	Application Purpose	Final Action Date	Lower Frequency In MHz	Upper Frequency In MHz
	Detail Summary			Long Range Systems Inc	4550 Excel Parkway #200	Addsion	TX	United States	75001	M74T7400	Original Equipment	03/24/2000	467.75	467.75

Perform Search Again

2 - Determine Modulation

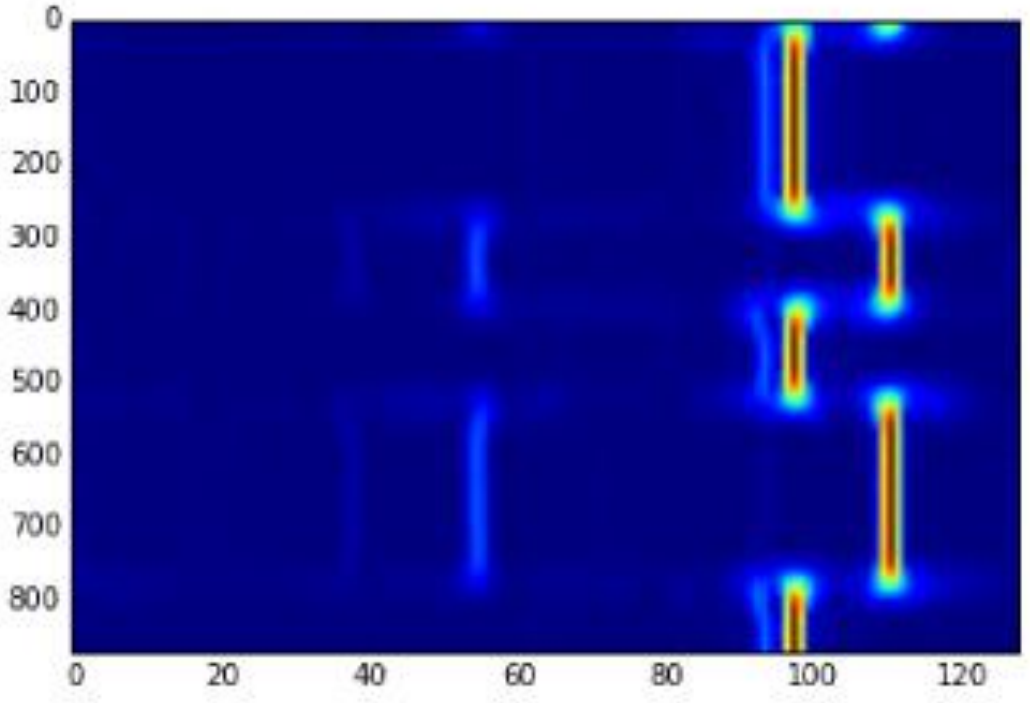
- Gqrx / inspectrum



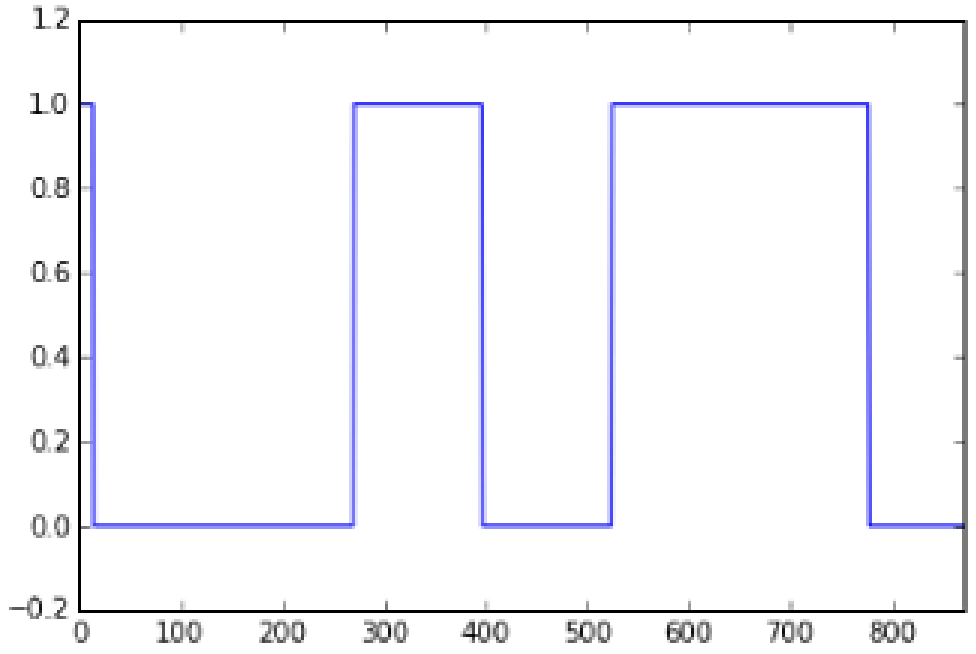
2 - Determine Modulation

- python

```
<matplotlib.image.AxesImage at 0x7ff896f484d0>
```

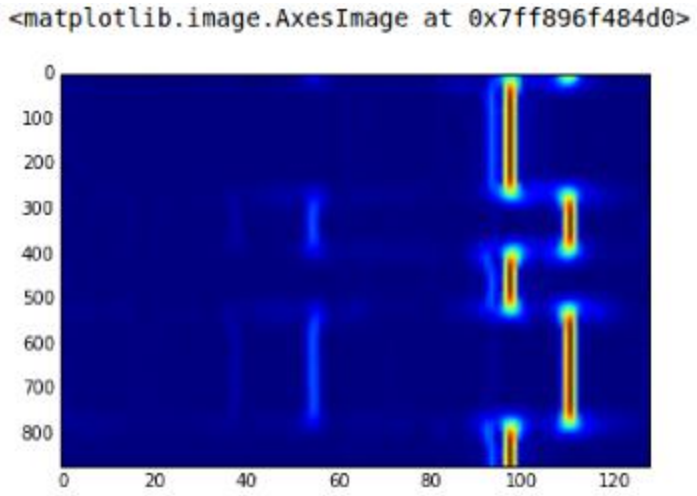


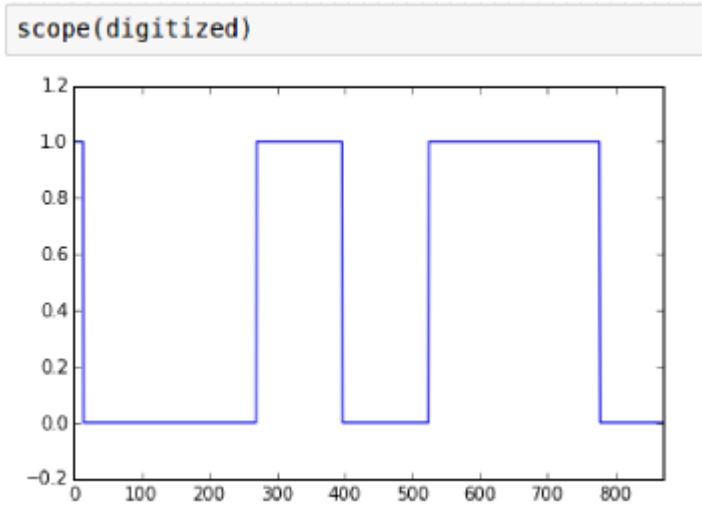

```
scope(digitized)
```

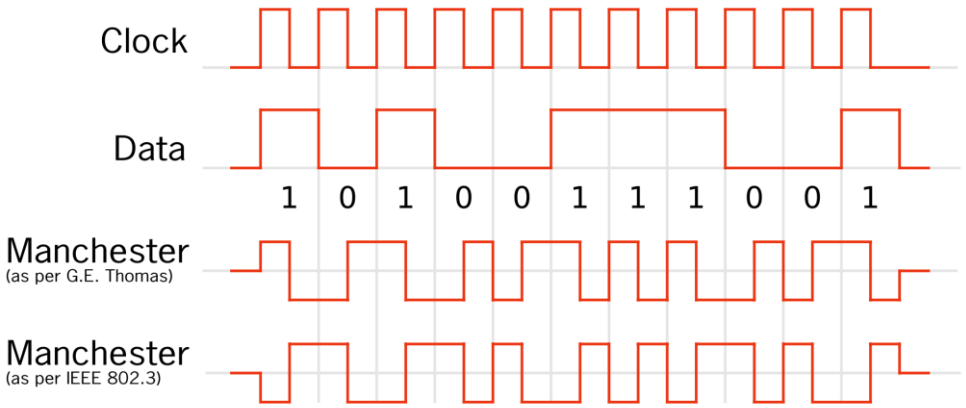


2 - Determine Modulation

- python







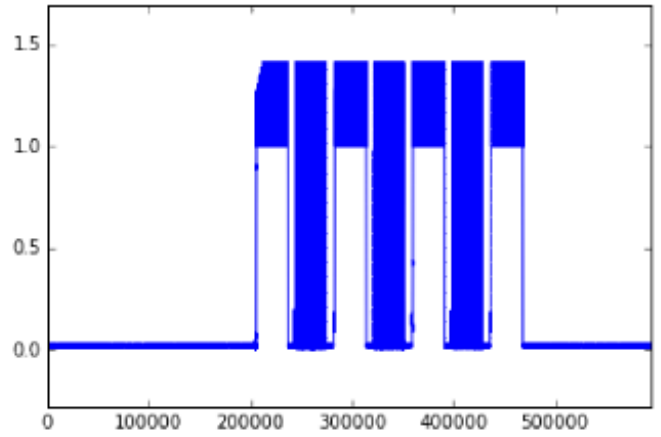
3 - Determine Protocol / Structure

- fc2d = preamble / header?
- 09 = function?
  - vibrate
  - lights
  - chime
  - all
- 0001 = pager id?
- 4478 = checksum?
- All those other bytes?

```
cs = decode_file('gqrx_20160314_pager1_467765000_80000_fc.raw')
[distillrfbase.hexsearch(c,'fc2d') for c in cs]
```

```
[BitStream('0xfc2d090001000000004478'),
 BitStream('0xfc2d0900010000000447, 0b100'),
 BitStream('0xfc2d090001000000004478'),
 BitStream('0xfc2d0900010000000447, 0b100'),
 BitStream('0xfc2d090001000000004478'),
 BitStream('0xfc2d0900010000000447, 0b100'),
 BitStream('0xfc2d090001000000004478')]
```

```
scope_file('gqrx_20160314_pager1_467765000_80000_fc.raw')
```



Conclusion

- SDR allows for cheaper barrier to entry when looking at RF
- Basic attacks work against some proprietary systems
  - Don’t rely on obfuscation
- Attack scenarios from traditional pentesting carries over to wireless
  - DoS
  - Fuzzing
  - Overflows
  - etc
- Dedicated hardware is still very useful for RE as the equipment was designed to work for that specific application
  - SDR might be the cheaper and/or only solution if black box testing

Questions?

Thanks and hack away!

- g@rrettgee.com
- http://garrettgee.com/lethal/
  - Slides
  - Links
  - Resources