SOFTWARE DEFINED RADIO

MIKE HAM

WHAT IS SDR?

- Effectively the goal is to remove the analog parts of a radio and do it all in software
  - Think about turning a knob on the radio and replacing that mechanism with software
- Rather than just being able to tune into one thing (e.g. FM radio), you can capture a wide array of bands

WHAT RADIO WAVES SURROUND YOU?

WHAT CAN SDR DO?

- This can be used as an AM / FM radio, a police scanner, air traffic control listener, etc.
- Receiver images from weather satellites
- You’re basically packet sniffing with radio
- Isn’t that not legit to do?
  - Use common sense when doing stuff like this
  - The antennas we have can only receive not transmit so we’re ok here

THE HARDWARE

- USB RTL-SDR Kit
- $17.99 from Hak5 http://hakshop.myshopify.com/collections/software-defined-radio/products/software-defined-radio-kit-rtl-sdr?variant=424034573

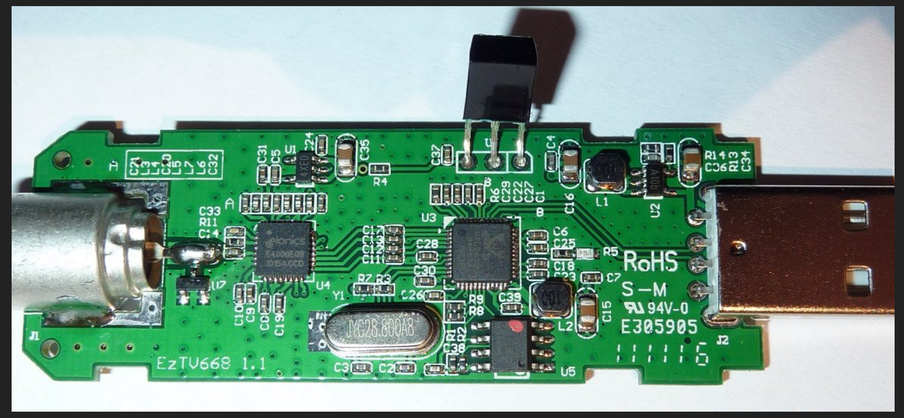
INTENDED PURPOSE

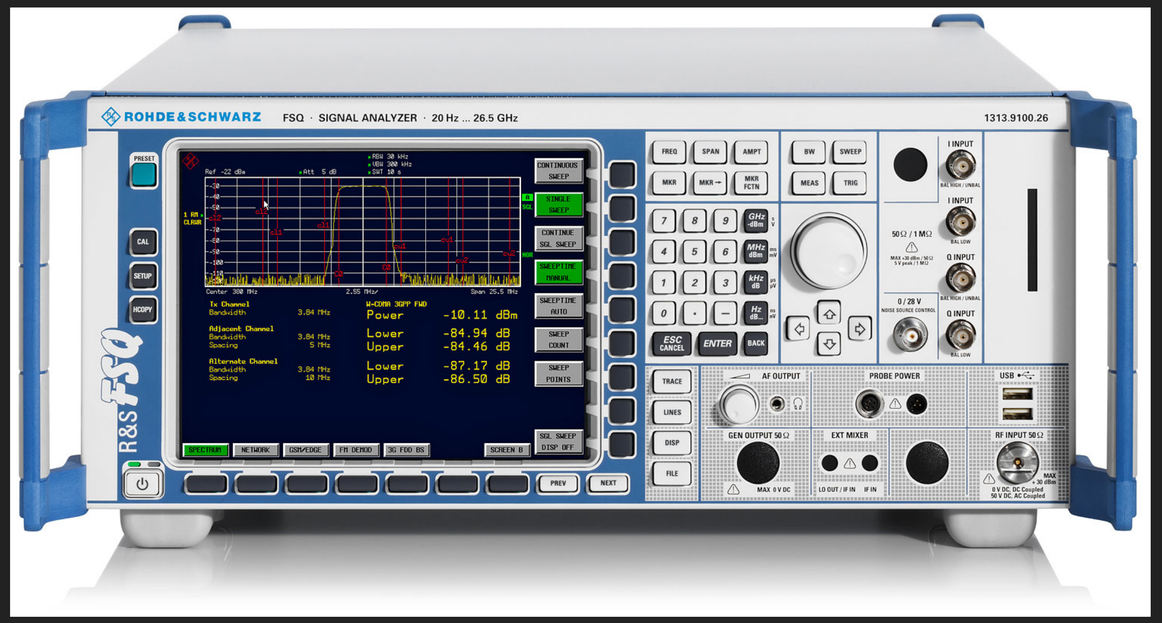
- This USD adapter is meant to allow users to record and watch digital TV on a computer
  - Still image snapshots, recording and playback, etc.
  - Play FM radio and DAB digital radio
- Realtek RTL2832U and R820T chipsets
  - With a little trickery, we can actually make these do a lot more

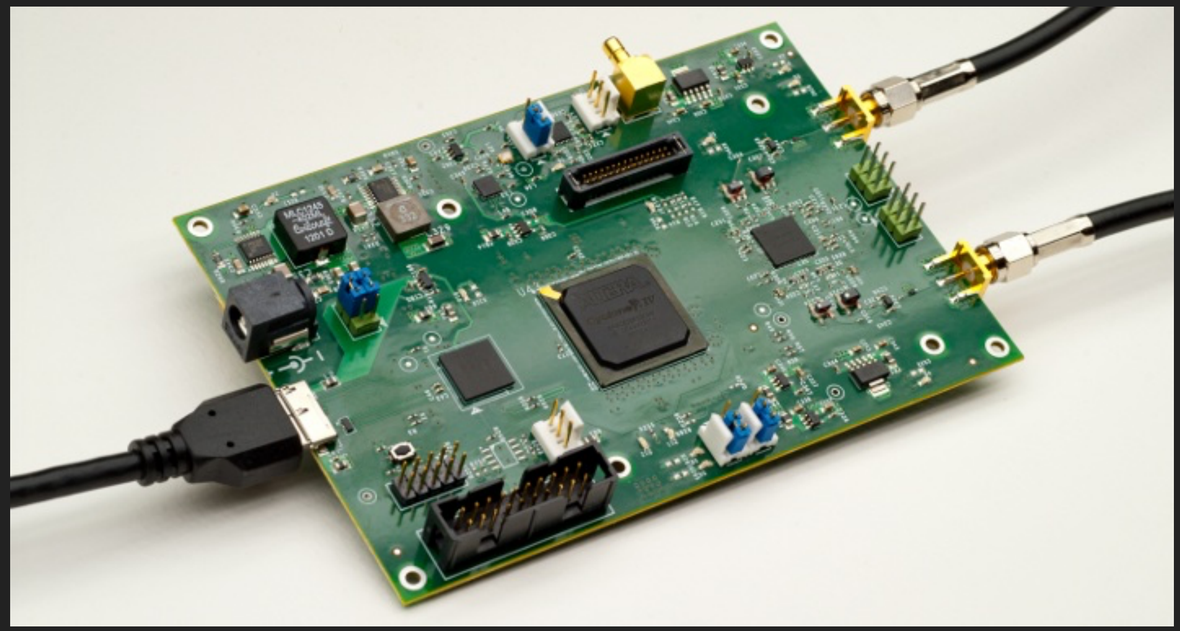
GEEKY SPECS

- DVBT:48.25 ~863.25 MHZ
- FM radio: 87.5~108 MHZ
- DAB radio: L-Band-1452960~1490624 KHZ
- VHF–174928~ 239200 KHz
- Will work for both for software defined radio and DVB video capture (where available)
- Compatible with most SDR software. Approx range: 25MHz-1700MHz
- 6-8 MHz Bandwidth

OTHER SDR HARDWARE

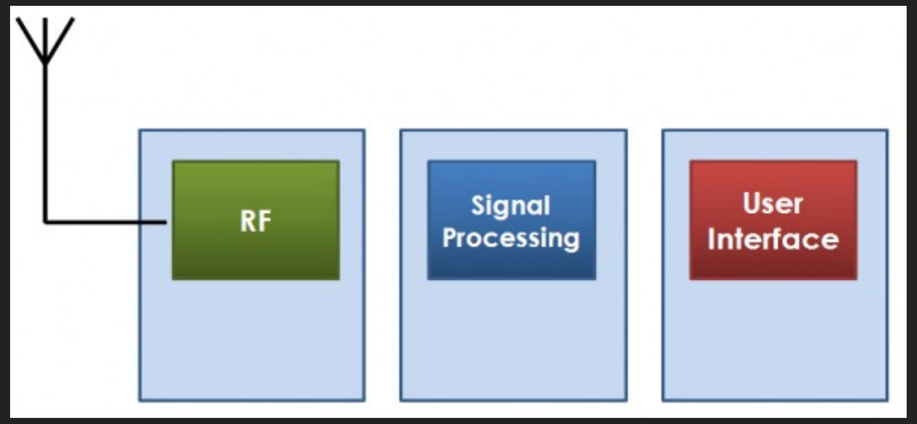




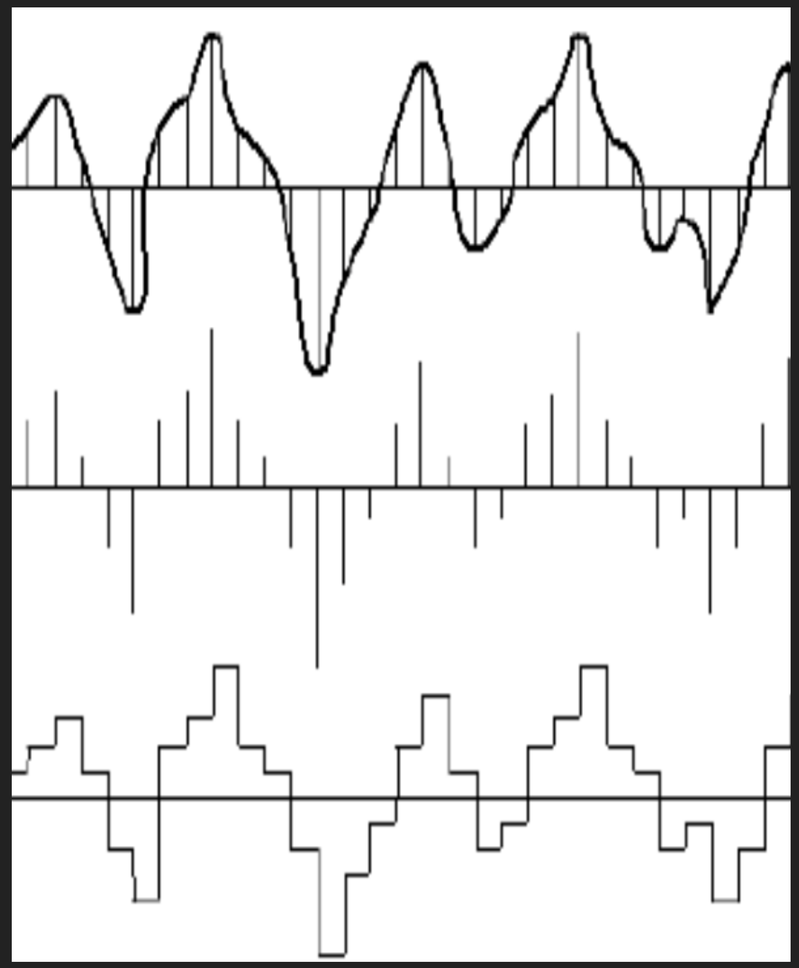


HOW DOES SDR WORK?

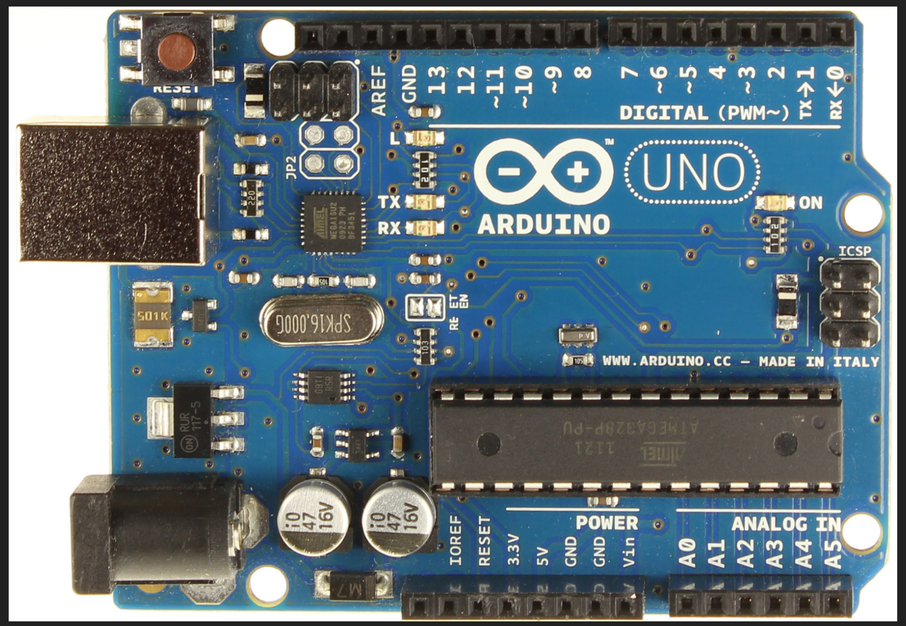
- At a 10,000’ view, SDR converts the analog signals on the antenna into digital signals (1’s and 0’s)
- Using signal processing techniques, we can make that data more usable



ORIGINAL → SAMPLED → RECONSTRUCTED



PRANKS?


UNO
ARDUINO
DIGITAL (PWM~)
POWER
ANALOG IN
WWW.ARDUINO.CC – MADE IN ITALY

+

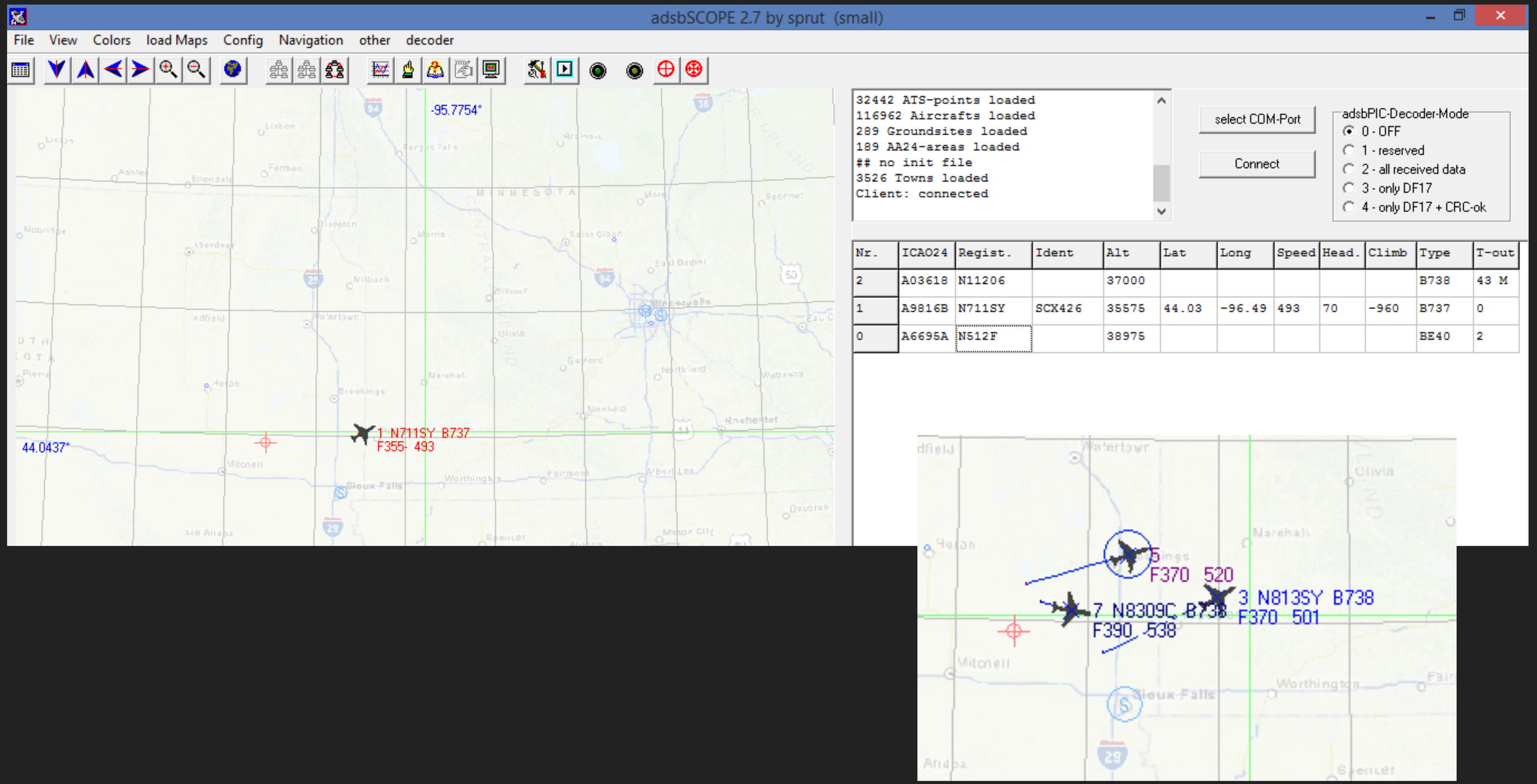
BALINT SEEBER — APPLICATIONS SPECIALIST

SOFTWARE DEFINED RADIO

OPENBTS

```
  == Using SIP RTP CoS mark 5
    -- Executing [222@sip-external:1] Macro("SIP/IMSI231082462443020
0000001", "dialGSM,IMSI231082462443019") in new stack
    -- Executing [s@macro-dialGSM:1] Dial("SIP/IMSI231082462443020-0
00001", "SIP/IMSI231082462443019") in new stack
  == Using SIP RTP CoS mark 5
    -- Called SIP/IMSI231082462443019
    -- SIP/IMSI231082462443019-00000002 is ringing
    -- SIP/IMSI231082462443019-00000002 is ringing
    -- SIP/IMSI231082462443019-00000002 is ringing
    -- SIP/IMSI231082462443019-00000002 is ringing
    -- SIP/IMSI231082462443019-00000002 is ringing
    -- Executing [600@sip-external:2] Echo("SIP/IMSI231082462443021-
000000", "") in new stack
    -- SIP/IMSI231082462443019-00000002 answered SIP/IMSI23108246244
20-00000001
    -- Locally bridging SIP/IMSI231082462443020-00000001 and SIP/IMS
31082462443019-00000002
```

SOFTWARE DEFINED RADIO



Nr.	ICAO24	Regist.	Ident	Alt	Lat	Long	Speed	Head.	Climb	Type	T-out
2	A03618	N11206		37000						B738	43 M
1	A9816B	N711SY	SCX426	35575	44.03	-96.49	493	70	-960	B737	0
0	A6695A	N512F		38975						BE40	2

JARED BOON

- Tire Pressure Monitoring System (TPMS)
- All cars in the US sold after 2008 have it
- We should know if one of our tires are low
- Guess what? There's no "wire" going into your tire to check the pressure, it's wireless

TPMS

- The signals have some really rudimentary protection on them, but Jared was able to demodulate them
- He could get each tire’s pressure from 30-50 feet away depending on the TPMS module
- Probably not a goldmine of information but interesting nonetheless

MORE IDEAS

- Building security badges
- Gated communities
- Doorbells
- Remote controlled power outlets

HACKING YOUR CAR KEYS

- EVERYTHING that transmits wirelessly should have an FCC ID on it
  - This includes your car key fob
  - Grab a couple of wireless things around you and see
- The FCC does extensive testing on these devices to learn how they work and to make sure that they operate safely within their design specification
- That info is publicly listed and searchable, so we too can figure out how stuff works