Software Defined Radio

“Just in case you forgot Layer 0 existed”

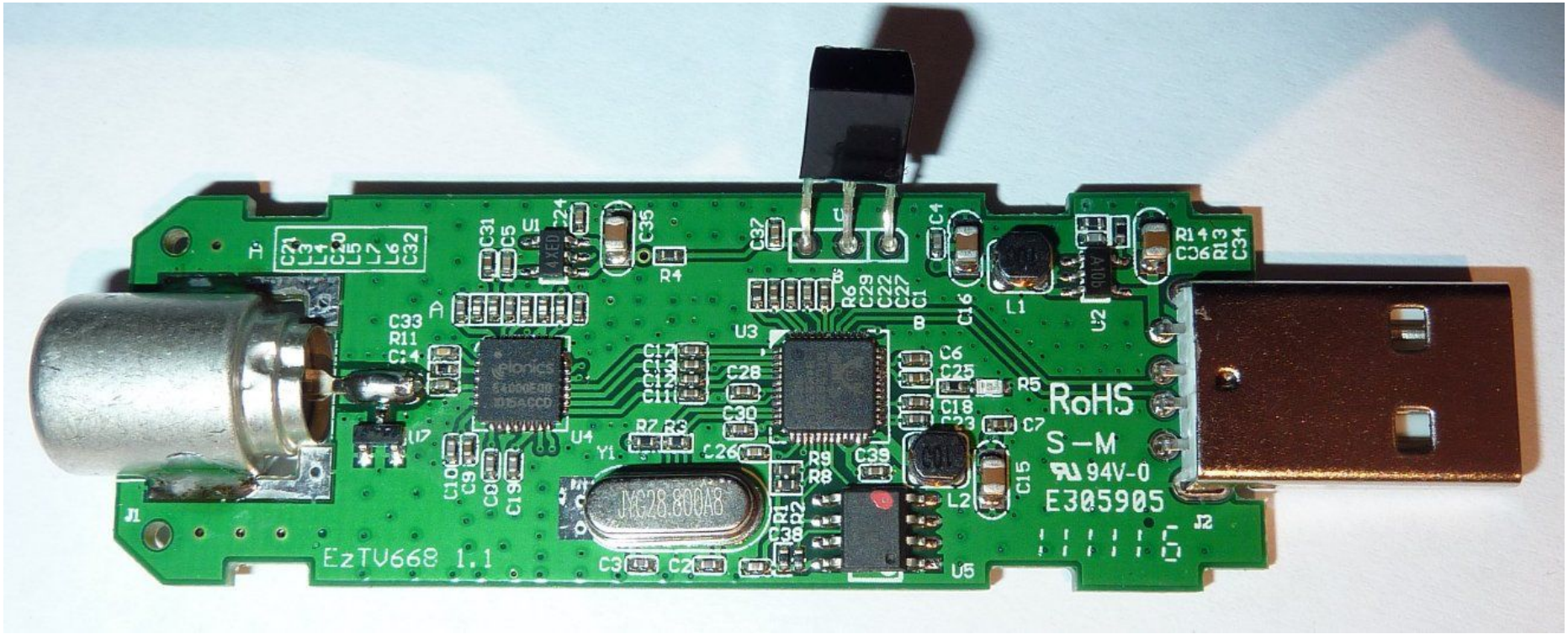
By Charlton Trezevant

$wtf is SDR

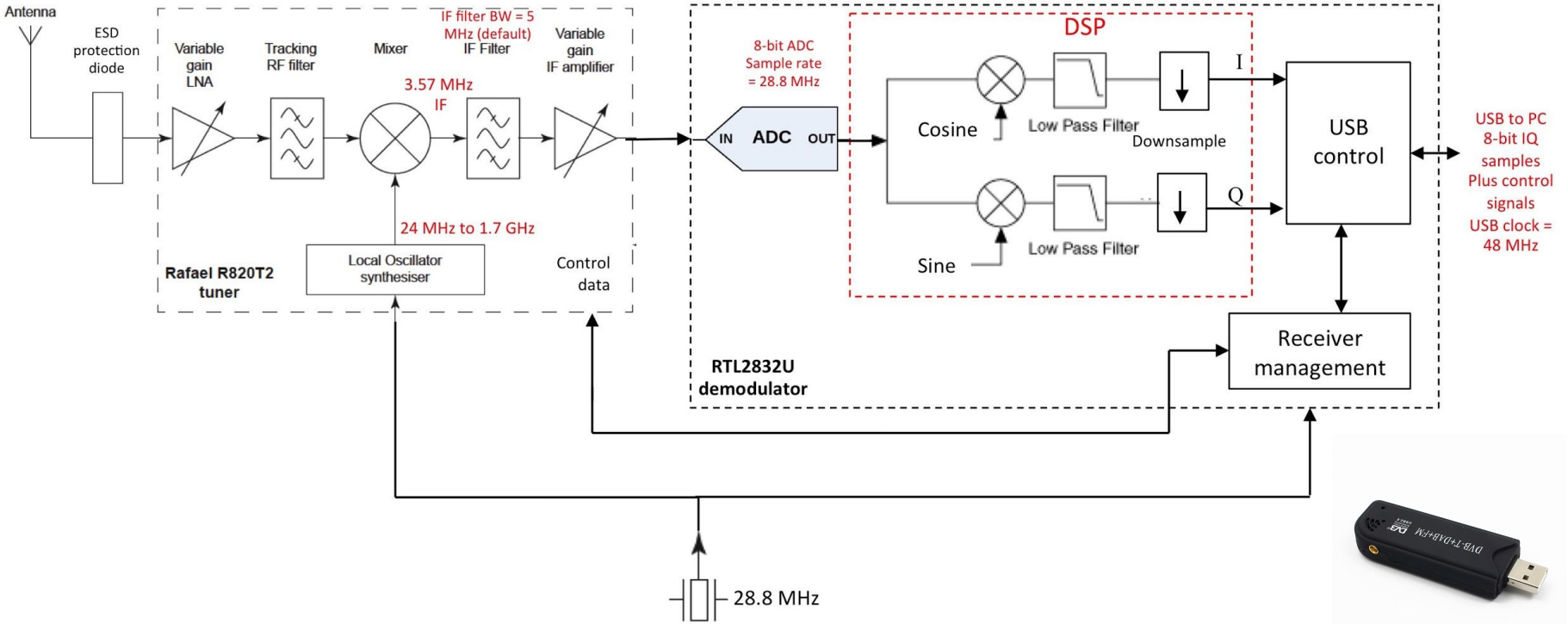
“**Software-defined radio (SDR)** is a radio communication system where components that have been traditionally implemented in hardware (e.g. mixers, filters, amplifiers, modulators/demodulators, detectors, etc.) are instead implemented by means of software on a personal computer or embedded system.”


METERS
METERS
EMERGENCY
ALARM
TRANSMITTER
MATCHING
MT-3000A
OMNI VI


147340
ICOM IC-V8000


EzTV668 1.1
RoHS
S-M
94V-0
E305905

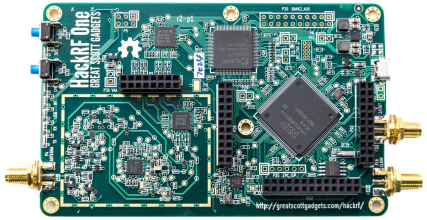
Simplified Block Diagram of NooElec RTL-SDR

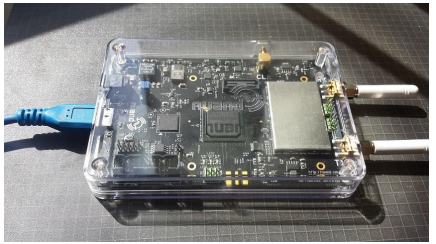


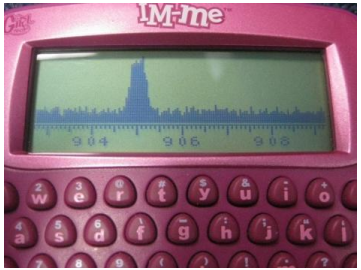
What you need to know

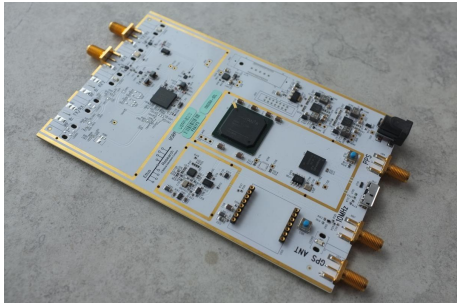
- Initially limited to people/institutions who could afford specialized (and expensive) spectrum analysis hardware, until relatively recently
- Cheap SDR is possible because China started pumping out DVB-T dongles based on the Realtek 2832U chipset
- Around 2010 RTLSDR was discovered as a driver was being developed to get those dongles working as regular TV/radio tuners in Linux
- RTLSDR dongles don’t transmit, but the more expensive SDR boards can
- Really useful for reverse engineering

Wide range of receiver equipment









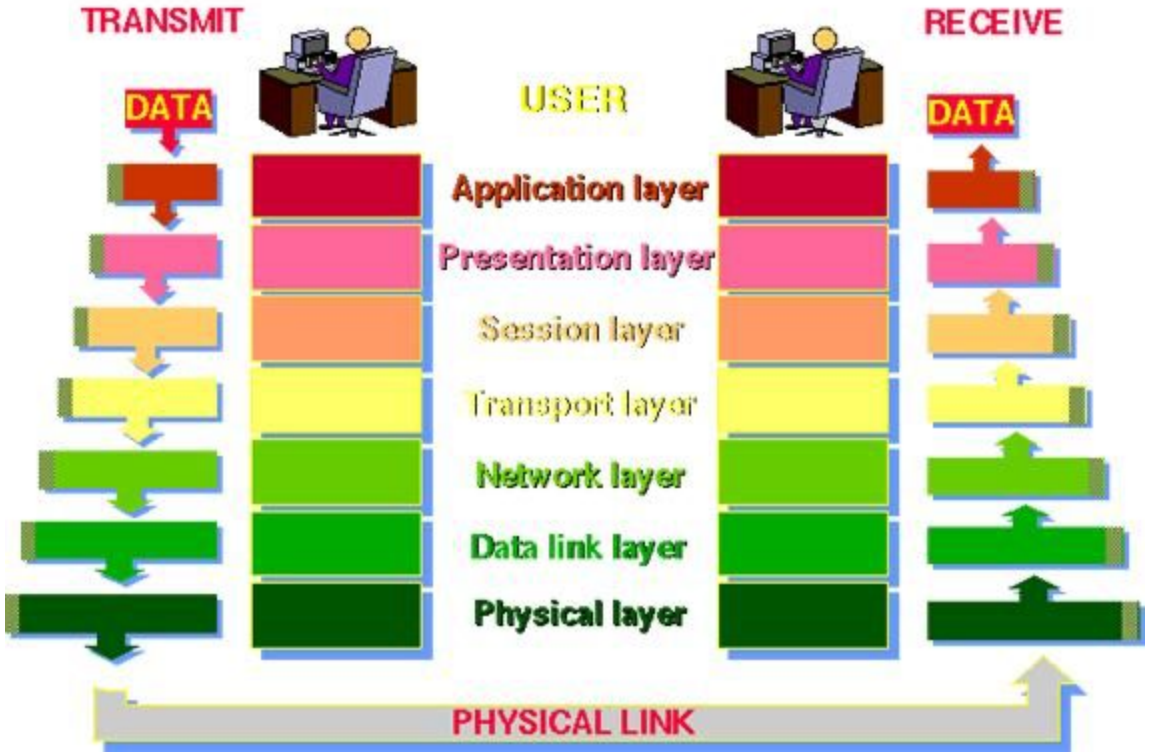
Rockchip-Based
DVB-T Dongles
(Cheap!)

Pro-Grade
(rich nerds ONLY!!1)

Modern devices have a bunch of radios

- GPS/GLONASS/Galileo
- 2G/3G/4G/LTE/5G
- WiFi (2.4Ghz + 5Ghz)
- Bluetooth 2-4.0 + BLE
- NFC/RFID
- Ultra Wideband
- AM/FM (sometimes)

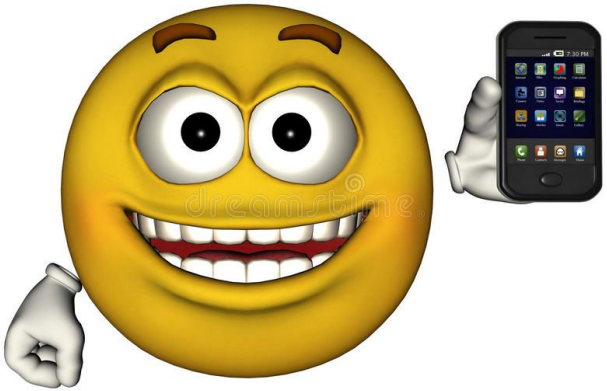
THE 7 LAYERS OF OSI



But what can I hack with it?

You can sniff literally anything that puts off RF, including:

- Bluetooth
- Cell phones
- Garage doors
- Eavesdropping on radio comms
- “IoT” devices
- NFC/RFID
- And much, much more



The only limit is the amount of spectrum your receiver can work with!

*Cheapo dongles generally have a range between ~24 - ~1750 MHz.

- *This can be extended with hardware mods, up/downconverters, otherwise no 2.4GHz*

But what can I hack with it? *contd.*

A few things you can listen to out of the box:

- Most voice communications
  - Think walkies, drive throughs, whatever. Both analog and trunked (TETRA/P25/etc)
- ADS-B/ACARS, AIS
  - Aircraft/ship positioning systems
- GSM/LTE
- GNSS
  - Positioning satellites
- NOAA satellites
  - Get the latest weather data right from the source
- Anything else in that entire huge frequency range

Where can I run it?

- Windows, Linux, OS X, Android
- Wide variety of software for every conceivable radio-related thing you may need
- Software also ranges in complexity from dead simple to ridiculous

Popular packages:

- GQRX
- SDR#
- URH (Universal Radio Hacker)
- Rtl_fm

FCC Registrations

“What if I want to listen to a specific thing?”

- Anything sold in the US that puts off RF is inspected by and registered with the FCC
- Any organization using RF (with the exception of a few reserved civilian bands) must register for a license from the FCC
- Conveniently, all of this information is public record and easily searchable!

Useful sites:

- wireless2.fcc.gov/UlsApp/UlsSearch/searchLicense.jsp
- www.radioreference.com
- www.fcc.gov/oet/ea/fccid
- fccid.io

License Search

Search Results

HELP

New Search | Refine Search | Printable Page | Query Download | Map Licenses

Specified Search

Name like **University of Central florida**
Status = **Active**

Matches 1- 10 (of 28)

PA = Pending Application(s)
TP = Termination Pending
L = Lease

Page 1 2 3 NEXT

	Call Sign/Lease ID	Name	FRN	Radio Service	Status	Expiration Date
1	KFO547	UNIVERSITY OF CENTRAL FLORIDA	0022163661	RP	Active	02/01/2021
2	KNIE248	UNIVERSITY OF CENTRAL FLORIDA	0007630148	PW	Active	01/13/2024
3	KNT99	UNIVERSITY OF CENTRAL FLORIDA	0022163661	TS	Active	02/01/2021
4	WHR493 L	University of Central Florida	0007630148	ED	Active	07/29/2027
5	WHR494 L	University of Central Florida	0007630148	ED	Active	02/04/2020
6	WKV20	UNIVERSITY OF CENTRAL FLORIDA	0022163661	TI	Active	02/01/2021
7	WLX309 L	University of Central Florida	0007630148	ED	Active	08/17/2020
8	WPKW651	UNIVERSITY OF CENTRAL FLORIDA	0007630148	IG	Active	08/18/2022
9	WPMQ646	UNIVERSITY OF CENTRAL FLORIDA	0007630148	IG	Active	11/06/2023
10	WPNR665	UNIVERSITY OF CENTRAL FLORIDA	0007630148	IG	Active	05/17/2024

Call Sign/Lease ID | Name | FRN | Radio Service | Status | Expiration Date

Page 1 2 3 NEXT

University of Central Florida

University of Central Florida (LTR) LTR Standard	Utilized by miscellaneous campus services.

Frequency	License	Type	Tone	Alpha Tag	Description	Mode	Tag
159.69000	WPPF903	RM	107.2 PL	UCF Bus-1	Shuttle Buses - Dispatch	FM	Schools
159.84000	WPPF903	RM	107.2 PL	UCF Bus-2	Shuttle Buses	FM	Schools
159.96000	WPPF903	RM	107.2 PL	UCF Bus-3	Shuttle Buses	FM	Schools
159.97500	WPPF903	M	103.5 PL	UCF Bus-4	Shuttle Buses - Talkaround	FM	Schools
451.72500	WPTS253	RM	072 DPL	UCF House	Maintenance - Housekeeping	FM	Schools
452.02500	WPTS253	RM	331 DPL	UCF Plumbing	Maintenance - Plumbing	FM	Schools
452.05000	WPTS253	RM	243 DPL	UCF Heat	Maintenance - Heating and Cooling	FM	Schools
452.20000	WPTS253	RM	532 DPL	UCF Maint	Maintenance	FM	Schools
452.65000	WPTS253	RM	072 DPL	UCF Grounds	Maintenance - Grounds	FM	Schools
463.70000	WQCF679	RM	123.0 PL	UCF Athletic	Athletics	FM	Schools
463.72500	WQCI630	RM	179.9 PL	UCF Rec Cntr	Recreation and Wellness Center	FM	Schools
464.30000	WPYS571	RM	311 DPL	UCF TRC	Technology Resource Center	FM	Schools
464.52500	WPWS397	RM	165 DPL	UCF Maint	Maintenance	FM	Schools
464.82500	WPRJ225	RM	118.8 PL	UCF Union	Student Union	FM	Schools
464.92500	WPRJ225	RM	146.2 PL	UCF Event	Student Union/ Event Services	FM	Schools

Dining Talkgroups

DEC	Mode	Alpha Tag	Description
0-11-002	A	Dining Svcs	Dining Services
0-11-008	A	Dining C Sto	Dining Services - C Store
0-11-009	A	Dining Svcs	Dining Services
0-11-010	A	Dining Cater	Dining Services - Catering

Football Stadium: Security & Events Team Talkgroups

DEC	Mode	Alpha Tag	Description	
0-19-003	A	Event Ops 1	Event Ops 1	
0-19-014	A	Event Ops 3	Event Ops 3	
0-19-022	A	Event Ops 4	Event Ops 4	Schools
0-15-007	A	EventParking	Event Parking	Security

FCC Callsign WQHI858 (UNIVERSITY OF CENTRAL FLORIDA)

Licensee Name:	UNIVERSITY OF CENTRAL FLORIDA
License:	WQHI858
FRN:	0007630148
Status:	Active (Effective: 05/26/2017 - Expires: 08/08/2027)
County:	ORANGE
State:	FL
Radio Service:	IG: Industrial/Business Pool, Conventional
Notes:	LIGHTINING DETECTION SYSTEM

FCC ID PAGTR-003

PAG-TR-003, PAG TR003, PAGTR-003, PAGTR-OO3

Kab Enterprise Co., Ltd. REMOTE CONTROL TR-003

FCC ID > Kab Enterprise Co., Ltd. > TR-003

An FCC ID is the product ID assigned by the FCC to identify wireless products in the market. The FCC chooses 3 or 5 character "Grantee" codes to identify the business that created the product. For example, the grantee code for **FCC ID: PAGTR-003** is **PAG**. The remaining characters of the FCC ID, **TR-003**, are often associated with the product model, but they can be random. These letters are chosen by the applicant. In addition to the application, the FCC also publishes ***internal images, external images, user manuals, and test results*** for wireless devices. They can be under the "exhibits" tab below.

Purchase on Amazon: REMOTE CONTROL

Application: REMOTE CONTROL

Equipment Class: DSC - Part 15 Security/Remote Control Transmitter

View FCC ID on FCC.gov: PAGTR-003

Registered By: Kab Enterprise Co., Ltd. - PAG (Taiwan)

you@youremail.com Subscribe

App #	Purpose	Date	Unique ID
	Original Equipment	2004-10-20	1WRZDFE+zgWh9l49JxMfZQ==

Operating Frequencies

Frequency Range	Rule Parts	Line Entry
314.6-315.4 MHz	15.231	1

Test Firm Information

Name of test firm and contact person on file with the FCC:
Firm Name: SPORTON International Inc
First Name: Kathy
Last Name: Lin
Telephone Number:886-2-2696-2468Extension:230
Fax Number: 886-2-2696-2255
E-mail: kathylin@sporton.com.tw

Applicant Information

Applicant's complete, legal business name:	Kab Enterprise Co., Ltd.
FCC Registration Number (FRN):	0011541562
Alphanumeric FCC ID:	PAGTR003
Unique Application Identifier:	1WRZDFE+zgWh9l49JxMfZQ==
Line one:	21-1 Fl., No. 33, Sec. 1
Line two:	Min Sheng Rd., Panchiao City
City:	New Taipei
State:	N/A
Country:	Taiwan
Zip Code:	220

Exhibits

All

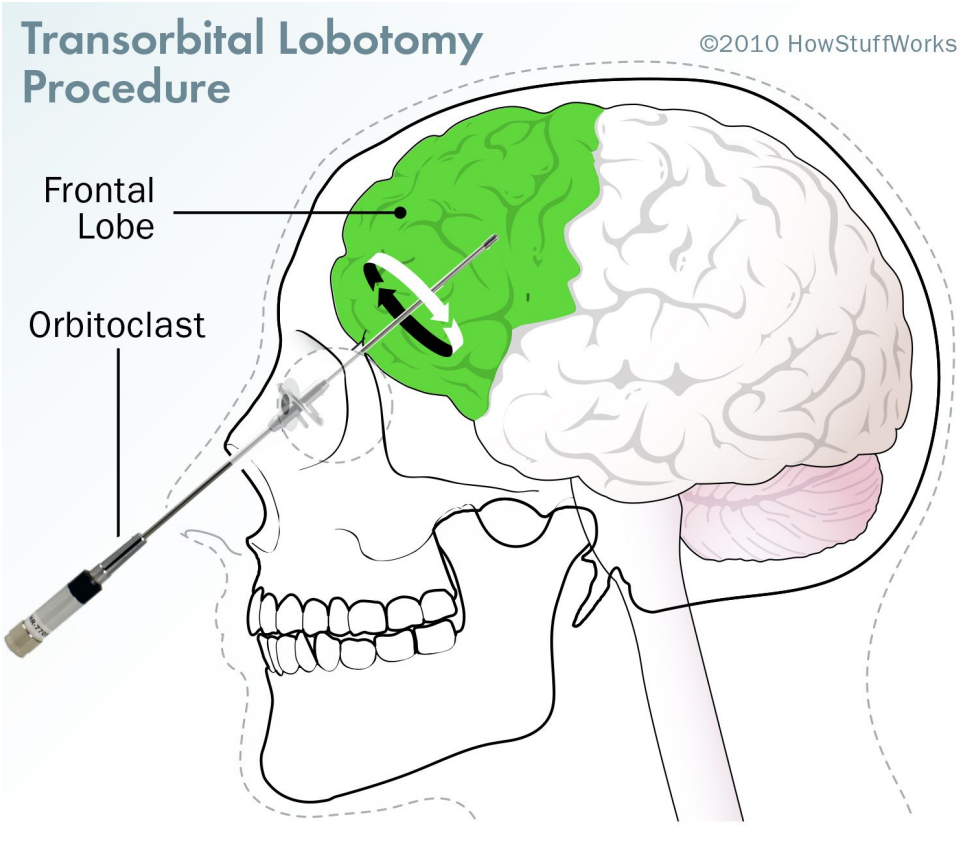
Document	Type	Submitted Available
USERS MANUAL	Users Manual Adobe Acrobat PDF (11 kB)	2004-10-20 2004-10-20
TEST SETUP PHOTOS	Test Setup Photos Adobe Acrobat PDF (341 kB)	2004-10-20 2004-10-20
TEST REPORT	Test Report Adobe Acrobat PDF (1938 kB)	2004-10-20 2004-10-20
INTERNAL PHOTOS	Internal Photos Adobe Acrobat PDF (120 kB)	2004-10-20 2004-10-20
ID LABLE LOCATION AND SAMPLE	ID Label/Location Info Adobe Acrobat PDF (67 kB)	2004-10-20 2004-10-20
EXTERNAL PHOTOS	External Photos Adobe Acrobat PDF (46 kB)	2004-10-20 2004-10-20
CONFIDENTIALITY LETTER	Cover Letter(s) Adobe Acrobat PDF (23 kB)	2004-10-20 2004-10-20
BLOCK DIAGRAM	Block Diagram Adobe Acrobat PDF (10 kB)	2004-10-20
OPERATIONAL DESCRIPTION	Operational Description Adobe Acrobat PDF (10 kB)	2004-10-20
SCHEMATICS	Schematics Adobe Acrobat PDF (78 kB)	2004-10-20

Application Forms

1 (2004-10-20)

Application for Equipment Authorization FCC Form 731 TCB Version

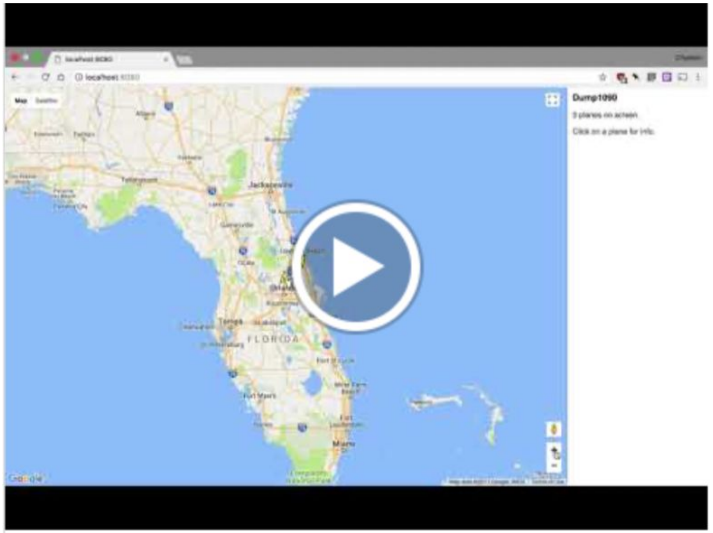
Demo Time!



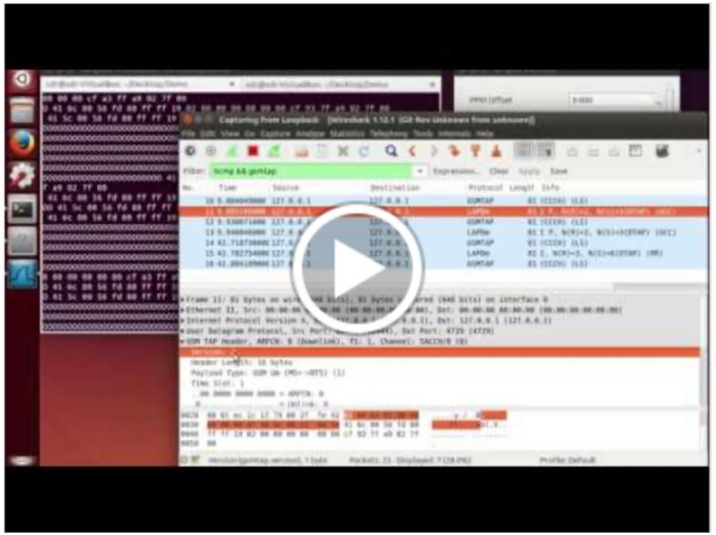
Extra info, links, demos, etc:

ctis.me/s/sdr

Demos



[Tracking planes with Dump1090]



[Sniffing GSM packets with GNURadio and Wireshark]