

WIRELESS SECURITY

IEEE/ACM PCJS CS Princeton Chapter, V1.1, March 17, 2016

TCF '41, 2016, V1.2, March 19, 2016

IEEE TCNJ Student Chapter V1.3, March 30, 2016

ADJUNCT PROF JOE JESSON

jessonj@tcnj.edu

Security Applications of Software Defined Radio

02/18/2018

HISTORY OF WIRELESS INTERCEPTION

- I. 1940's WWII WIRELESS SECURITY
- II. 1950's – 1960's COLD WAR COMMUNICATIONS
- III. 1980 – 2016 COMMERCIAL CELLULAR, WIFI, SATELLITE INTERCEPTION
- IV. 2010-2016 SPECTRUM SOFTWARE DEFINED REVOLUTION BEGINS
 - II. REALTEK SDR (RTL-SDR) & EXAMPLES
 - III. HACKRF SDR TRANSMIT & EXAMPLES
- V. LATEST WIRELESS SECURITY DEVELOPMENTS

WWII BLECHLEY PARK – READ GERMAN MESSAGES

RADIO INTERCEPTION

"Y"-Operators copy Morse Code
5-Character Sets, 3-Char Routing



ANALYSIS OF INTERCEPTED TRAFFIC

"Y"-Operators Analyze Radio Person Pattern/Frequency

BREAKING OF ENIGMA KEY

Determine New Key, Turing-Welchman Bombe



DECODING MESSAGES

CRIBs Limit Search Space, Language Translation

EXTRACTING INTELLIGENCE

Traffic Analysis, Logistics Flow, Mapping Context, Saved 2 Years!

WWII BLECHLEY PARK – READ GERMAN MESSAGES

WWII “Y”-OPERATOR INTERCEPT STATION
RCA AR-88 HF RECEIVER

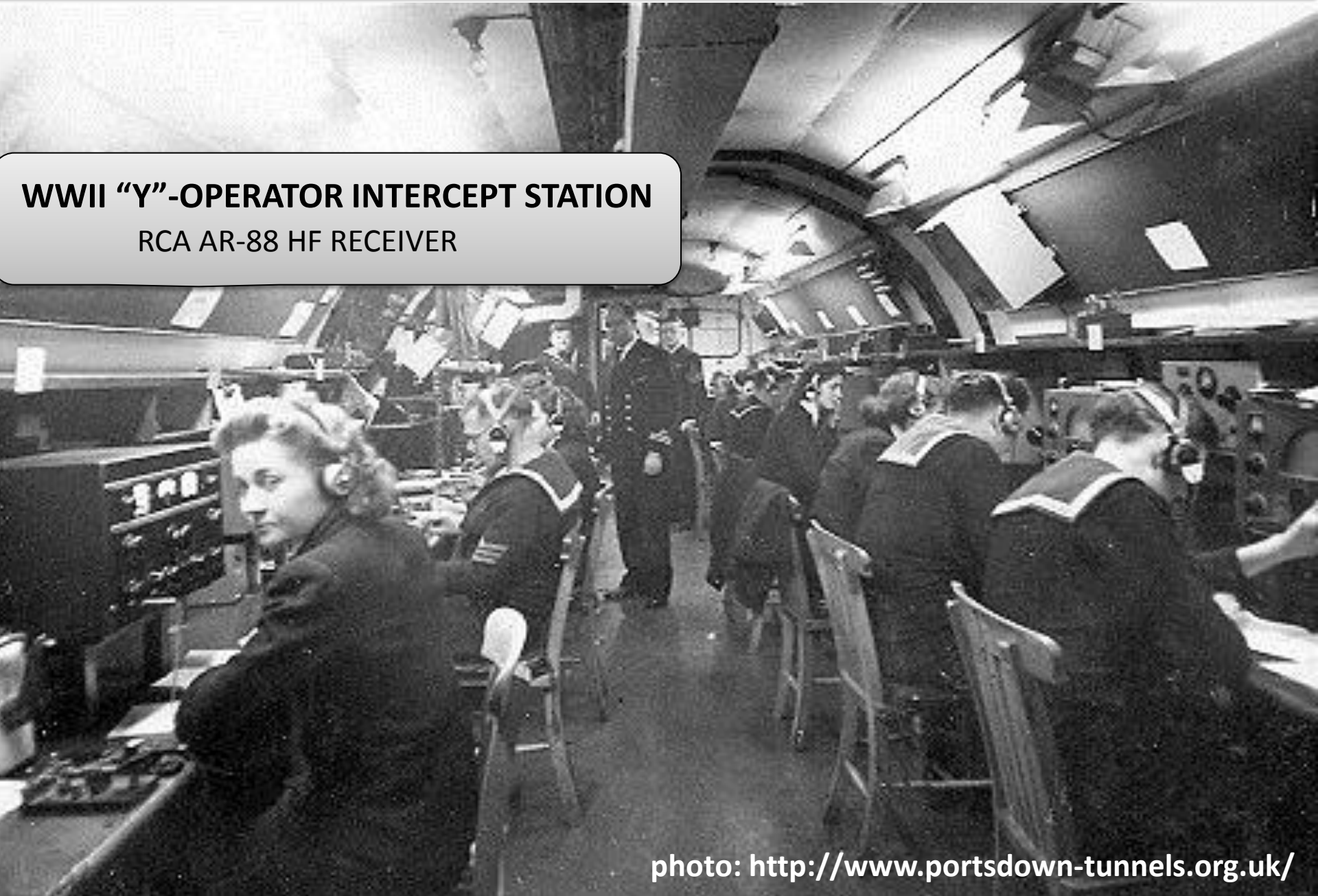


photo: <http://www.portsdown-tunnels.org.uk/>

Wireless Communications Security WWII [2]

RCA AR-88 RADIO INTERCEPTION [3-0]

- FAVORITE INTERCEPTION RECEIVER - DESIGNED GOAL, "BEST DESIGN, COST IS NO OBJECT"
- MANUFACTURED IN CAMDEN, NJ - SOME UNITS MFG IN CANADA, BRAZIL, FRANCE, UK

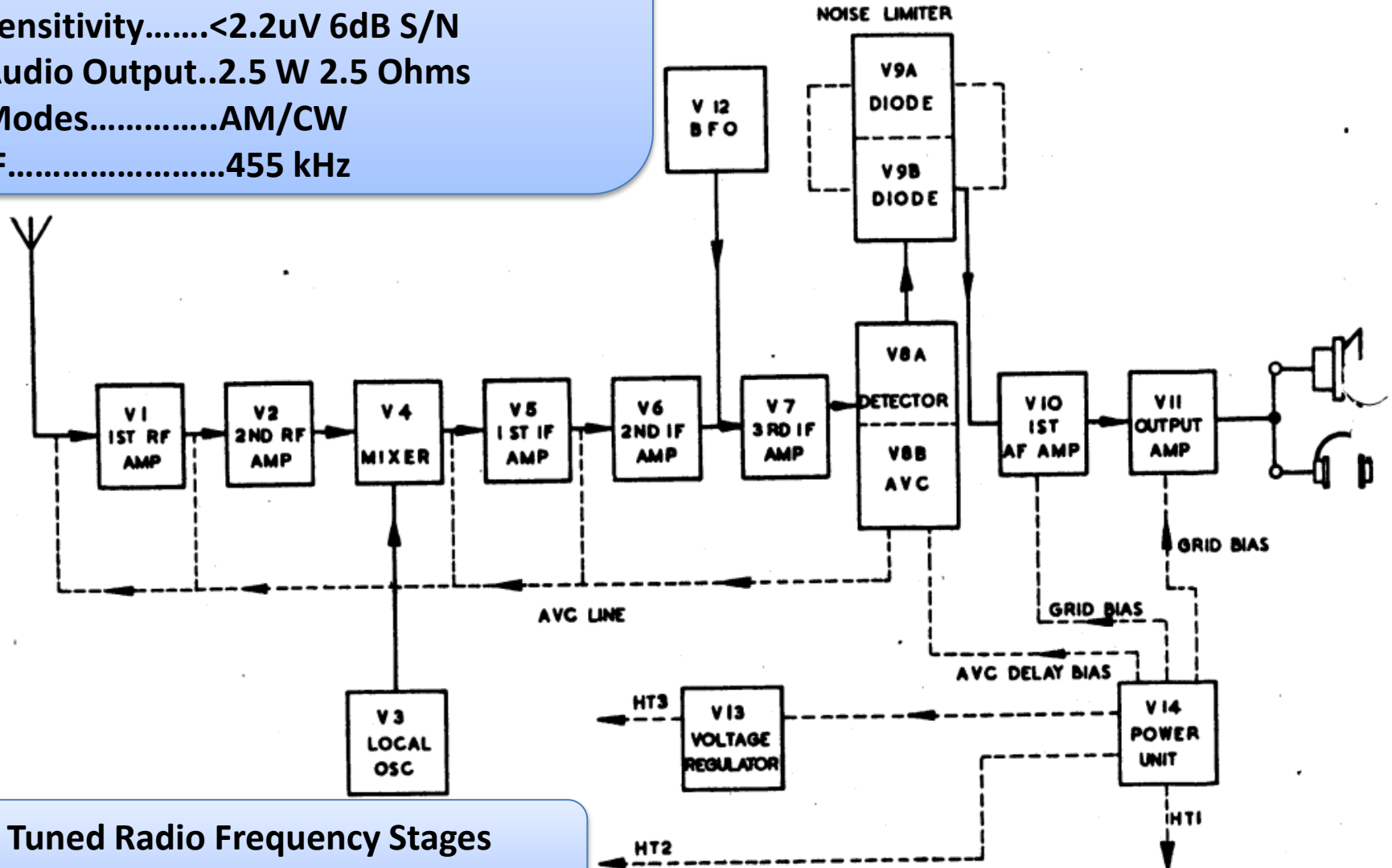


photo: <http://www.radioblvd.com/ar88.htm>

RCA AR-88 ARCHITECTURE [1] [3]

RCA AR-88 SPECIFICATIONS [1]

- Coverage.....535 – 32000 kHz
- Selectivity.....13.5/7/2.5/1/.5 kHz -6dB
- Sensitivity.....<2.2uV 6dB S/N
- Audio Output..2.5 W 2.5 Ohms
- Modes.....AM/CW
- IF.....455 kHz



Two Tuned Radio Frequency Stages

RECEIVER WITH PAN DISPLAY 1970's WATKINS-JOHNSON

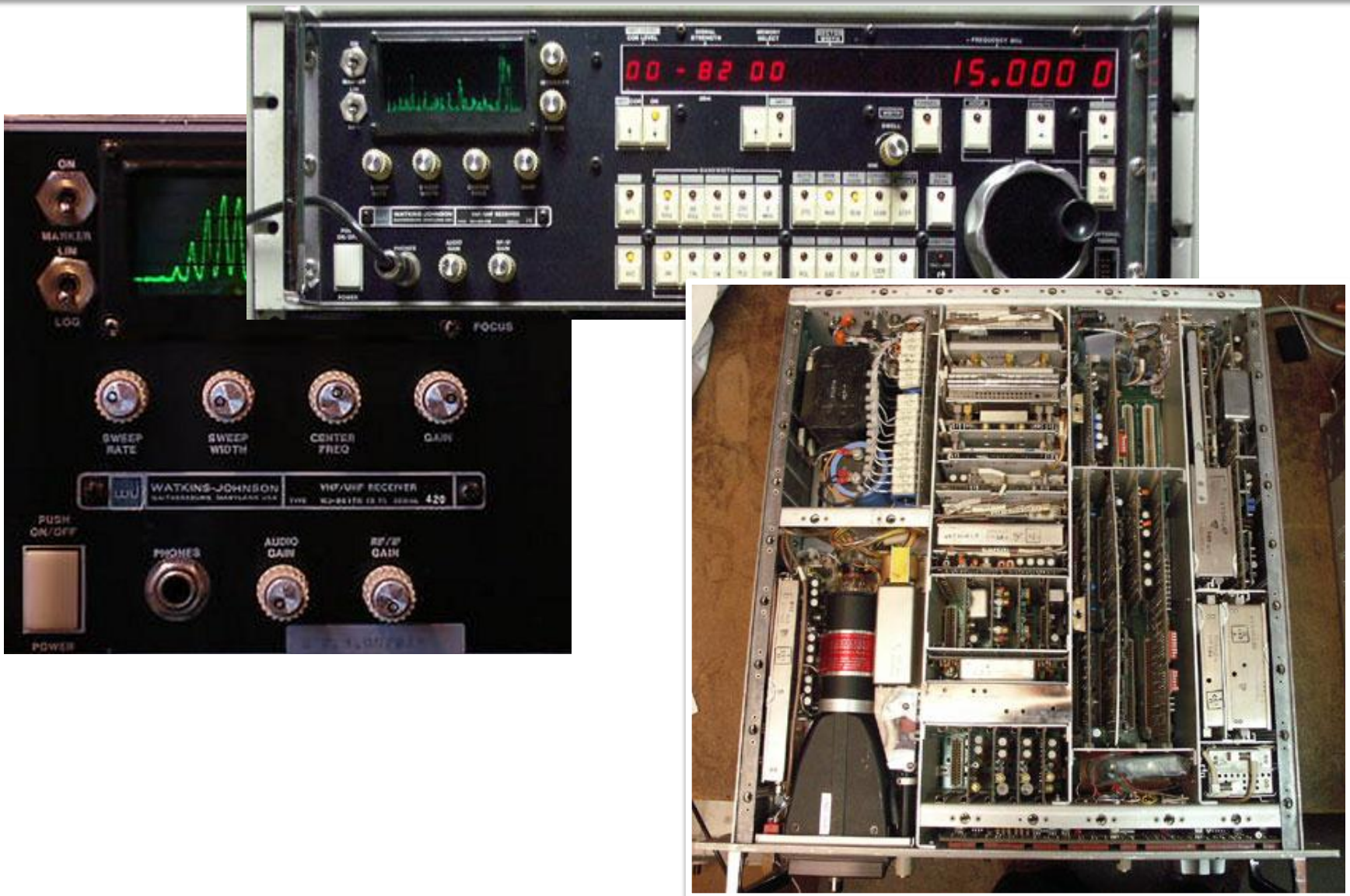
WATKINS-JOHNSON, GOVERNMENT MONITORING

- NON-ENCRYPTED NARROW-BAND FM (NBFM) BUG MONITORING
- WATERGATE EVIDENCE (EXIT RICHARD NIXON)



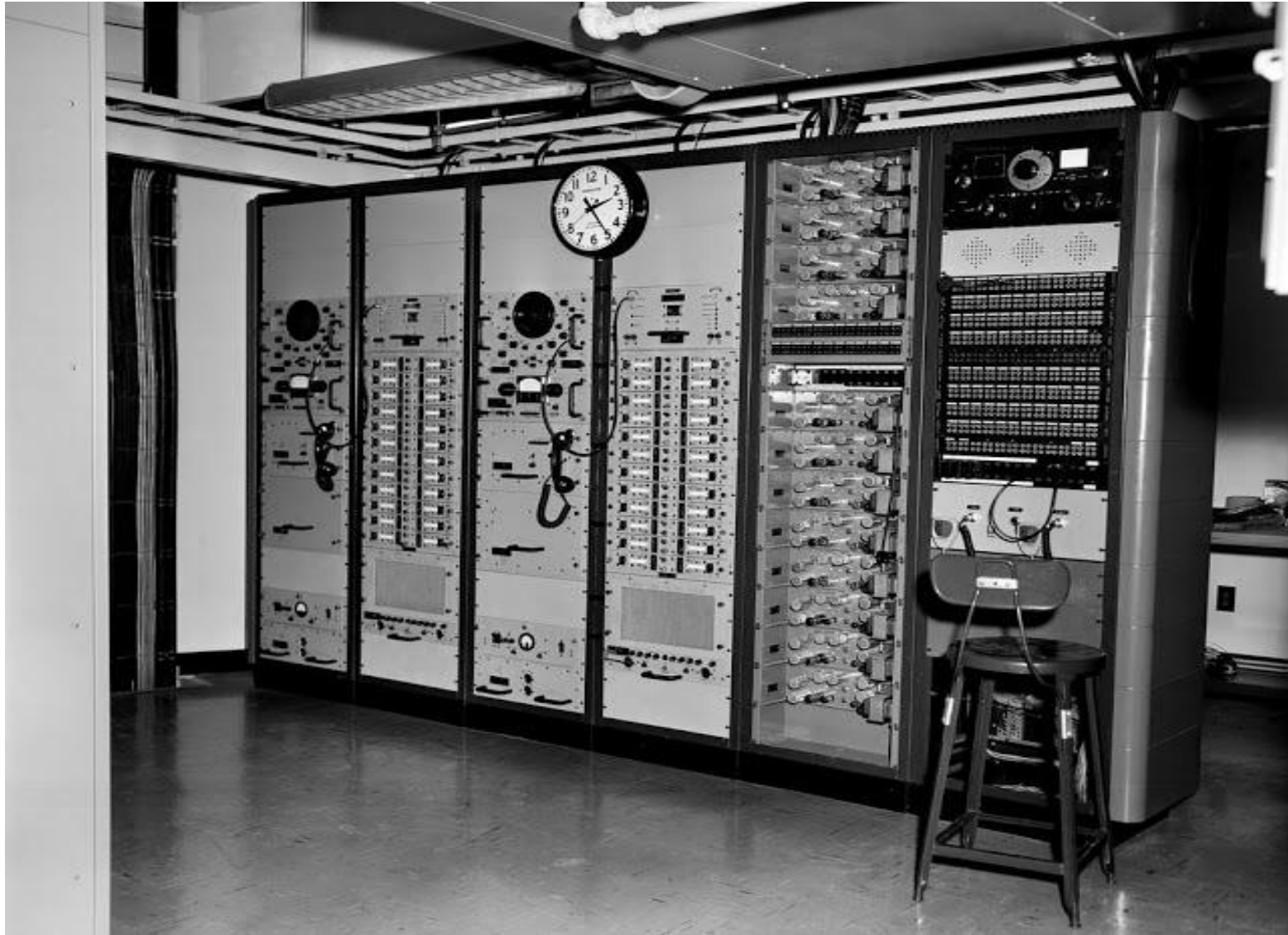
RECEIVER WITH PAN DISPLAY 1980's WATKINS-JOHNSON

EMBASSY COMMUNICATIONS, 1990's WITH SPECTRUM DISPLAY



White H*use Comm, 1970's Frederick MUX

AF*1, AF*2 ENCRYPTED (SOMETIMES) MUX VOICE COMMUNICATIONS



White H*use Comm, 1993 Frederick MUX

Technical Surveillance and Counter Measures Equipment (TSCM)

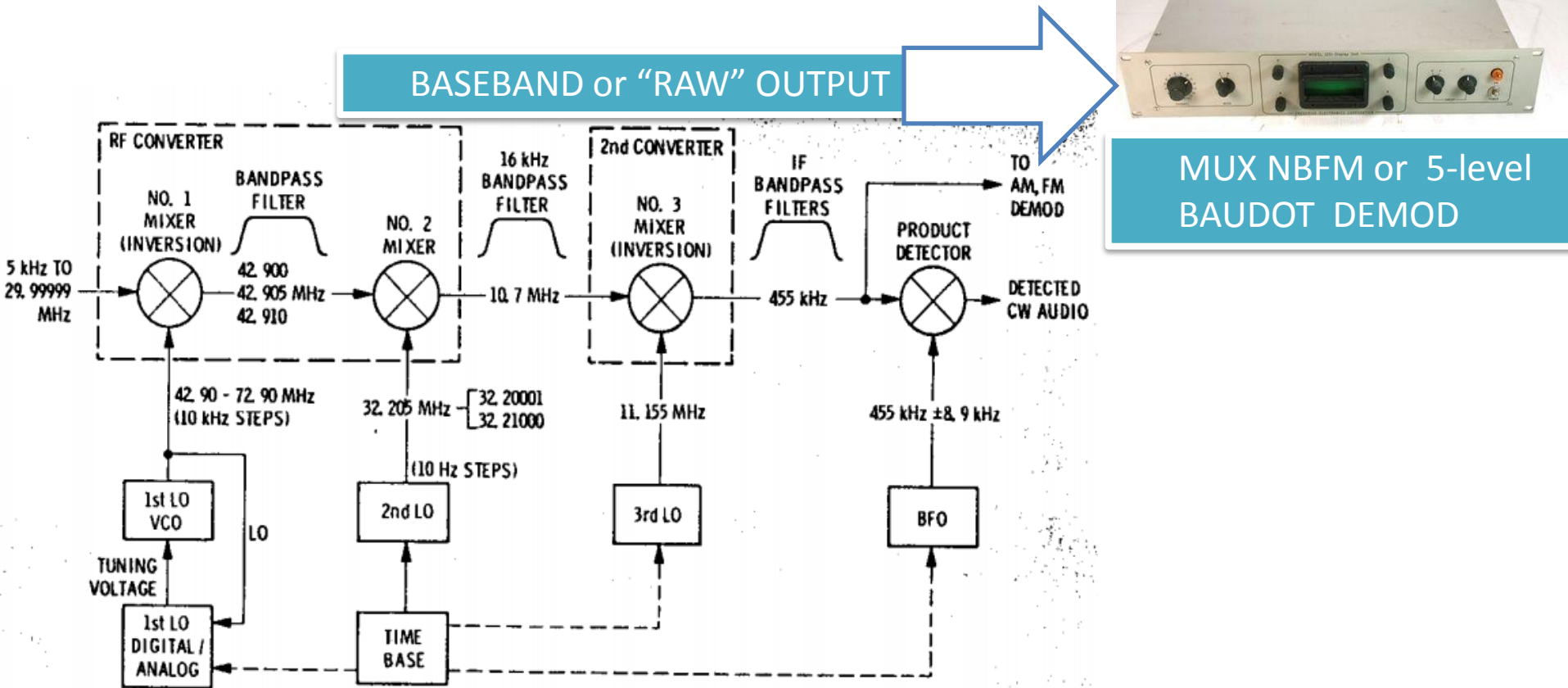


Figure 1. Digitally-controlled HF receiver frequency plan.



MUX NBFM or 5-level
BAUDOT DEMOD

ENCRYPTION OFTEN TOGGLED OFF (!) DUE TO
SYNCHRONIZATION LOST & GARBLED VOICE

TSCM, 1970's => 1990 MASON

Technical Surveillance and Counter Measures Equipment (TSCM)



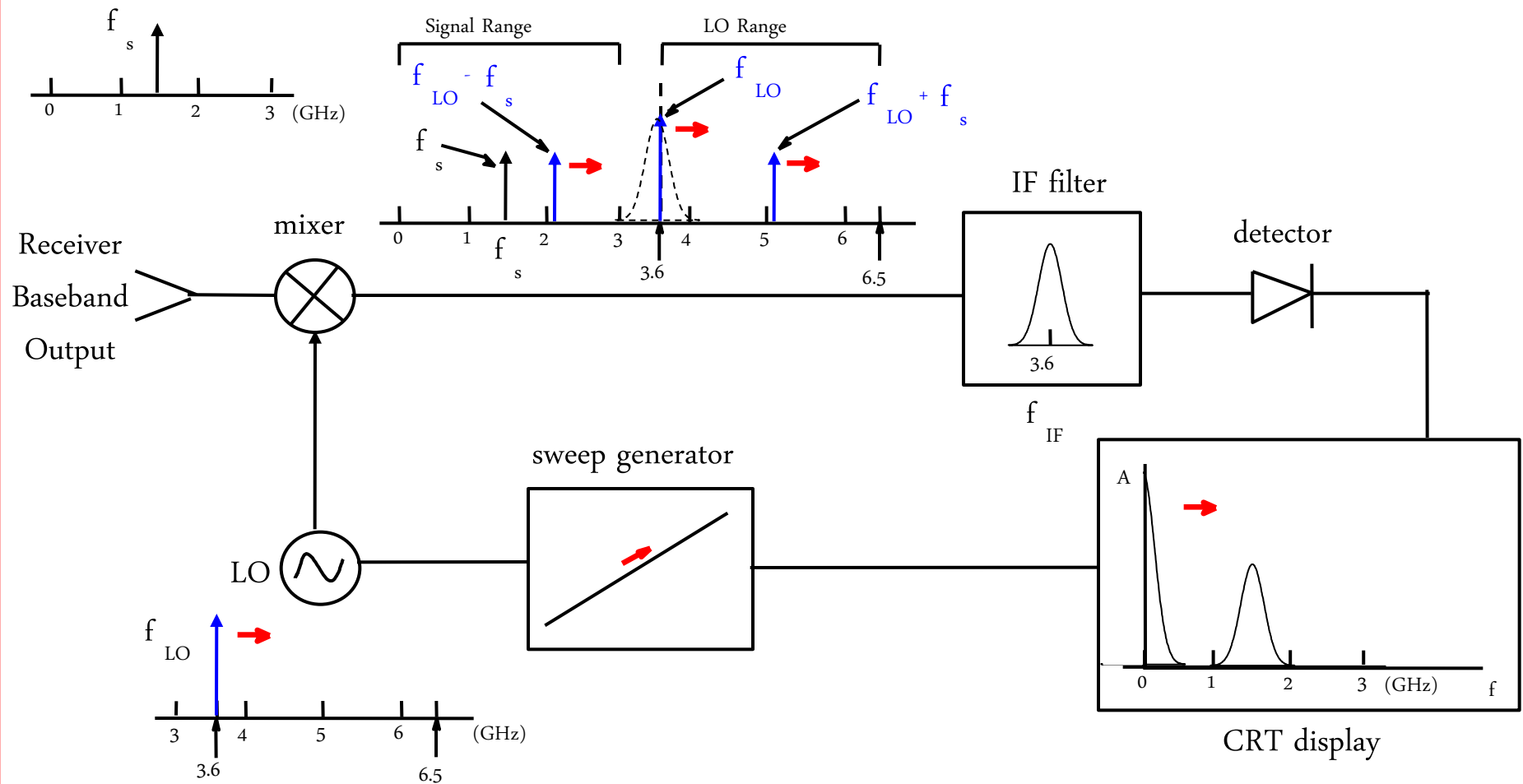
MASON A3 1971 Portable Intercept



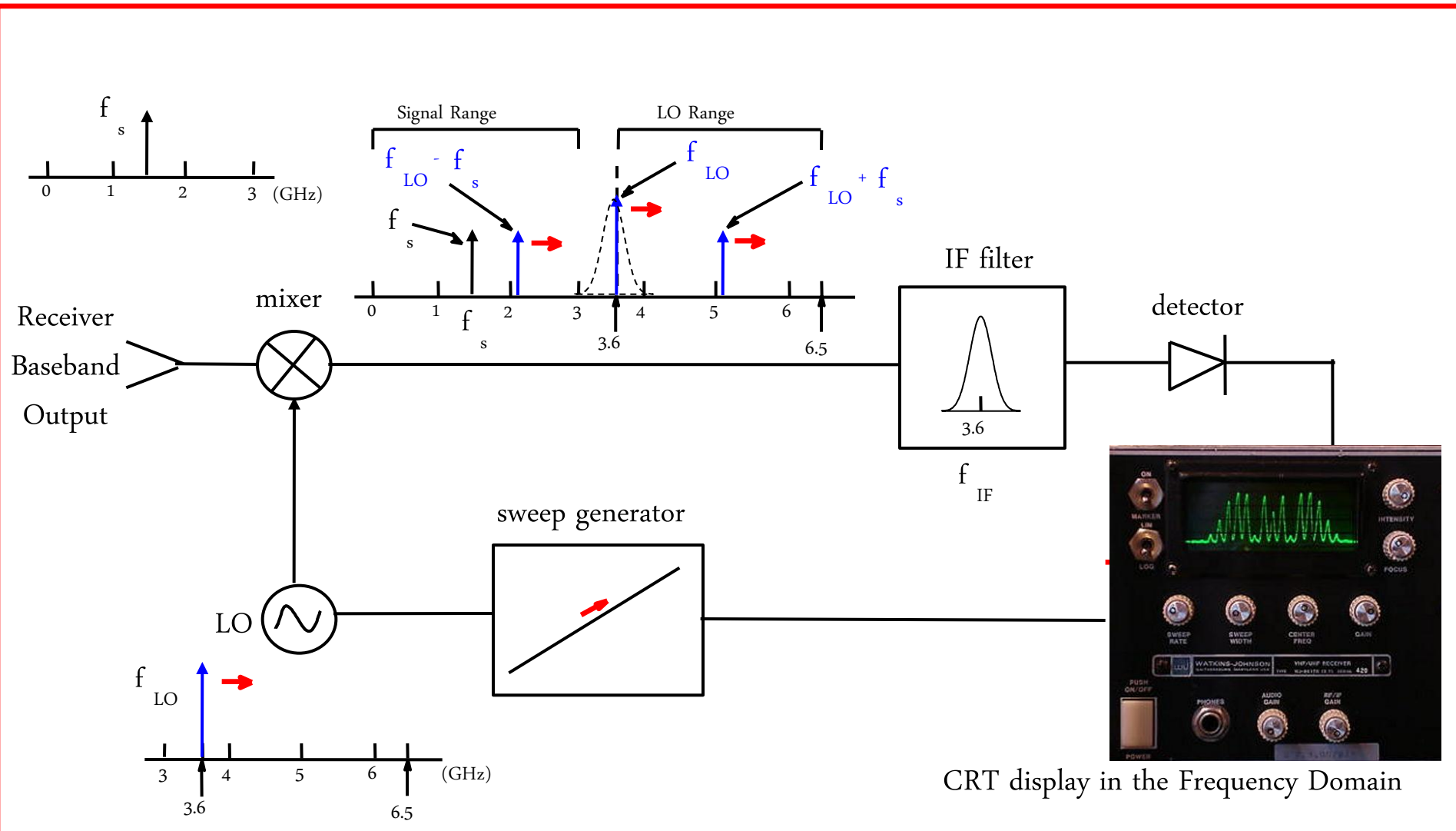
MASON MPR-1 Portable Intercept

Wireless Security Architecture – Freq Display

PANARAMIC SWEPT FREQUENCY DISPLAY



Wireless Security Architecture – Freq Display



ANALOG SWEPT SPECTRUM DISPLAY

Spread Spectrum - Frequency Hopping

[SINCGARS](#) family of US Combat Radio products. It supports (slow) **Frequency Hopping** (FH) and is backwards compatible with Single Channel radios.

the RT-1439 is a non-ICOM device. For the transmission of secure communication (voice and data) an external COMSEC device, such as the [KY-57 \(Vinson\)](#) or the [KY-99](#), is needed. COMSEC devices are connected to the 6-pin [U-229 audio sockets](#) (U-329/U) on the front panel.



Reference Site: <http://www.cryptomuseum.com/index.htm>

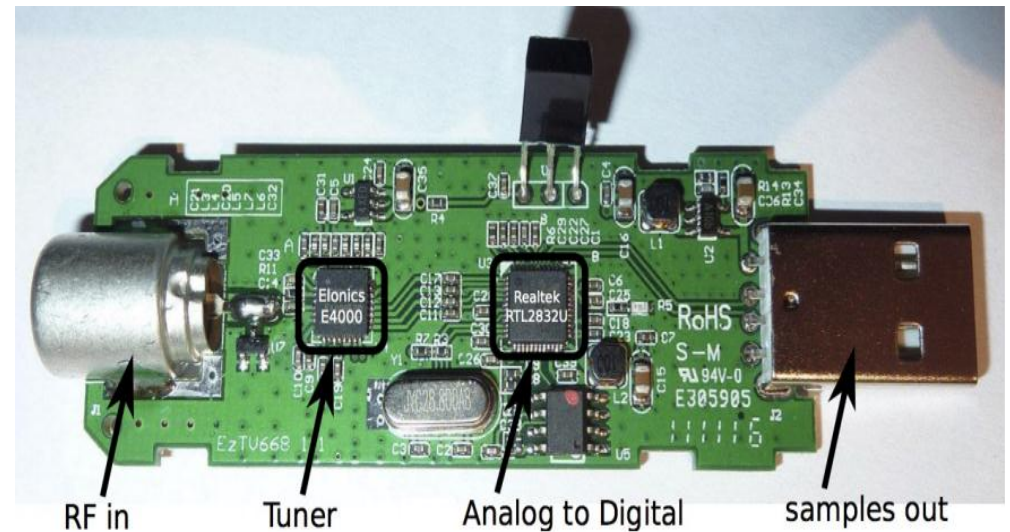
SPECTRUM DISPLAY, 1980's, MATHEMATICAL SYSTEMS DESIGN - FFT

NOTICE THE TEMPEST SCREENED DISPLAY



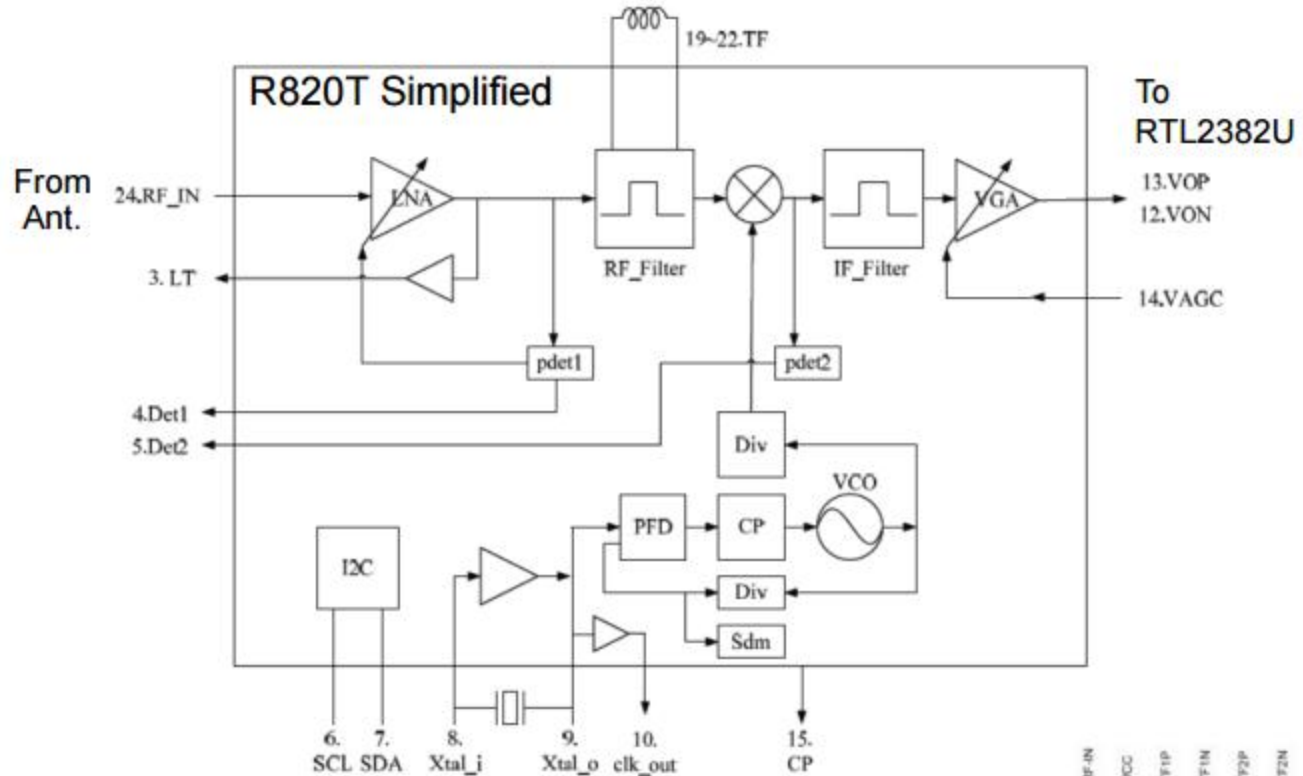
THE REVOLUTION BEGINS 2010-2012 RTL-SDR [4]

RTL-SDR is a very cheap software defined radio that uses a DVB-T TV tuner dongle based on the RTL2832U chipset. Antti Palosaari, Eric Fry and Osmocom (2010-2012) it was found that the signal I/Q data could be accessed via the USB port, which allowed the DVB-T TV tuner to be converted into a wideband software defined radio via a new software driver.



RF / IF INTEGRATED CIRCUIT, IN RTL-SDR [4]

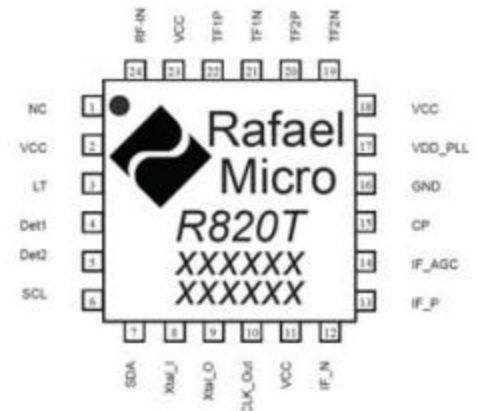
RF / IF IC, RAFAEL MICRO R820T



Typical figures

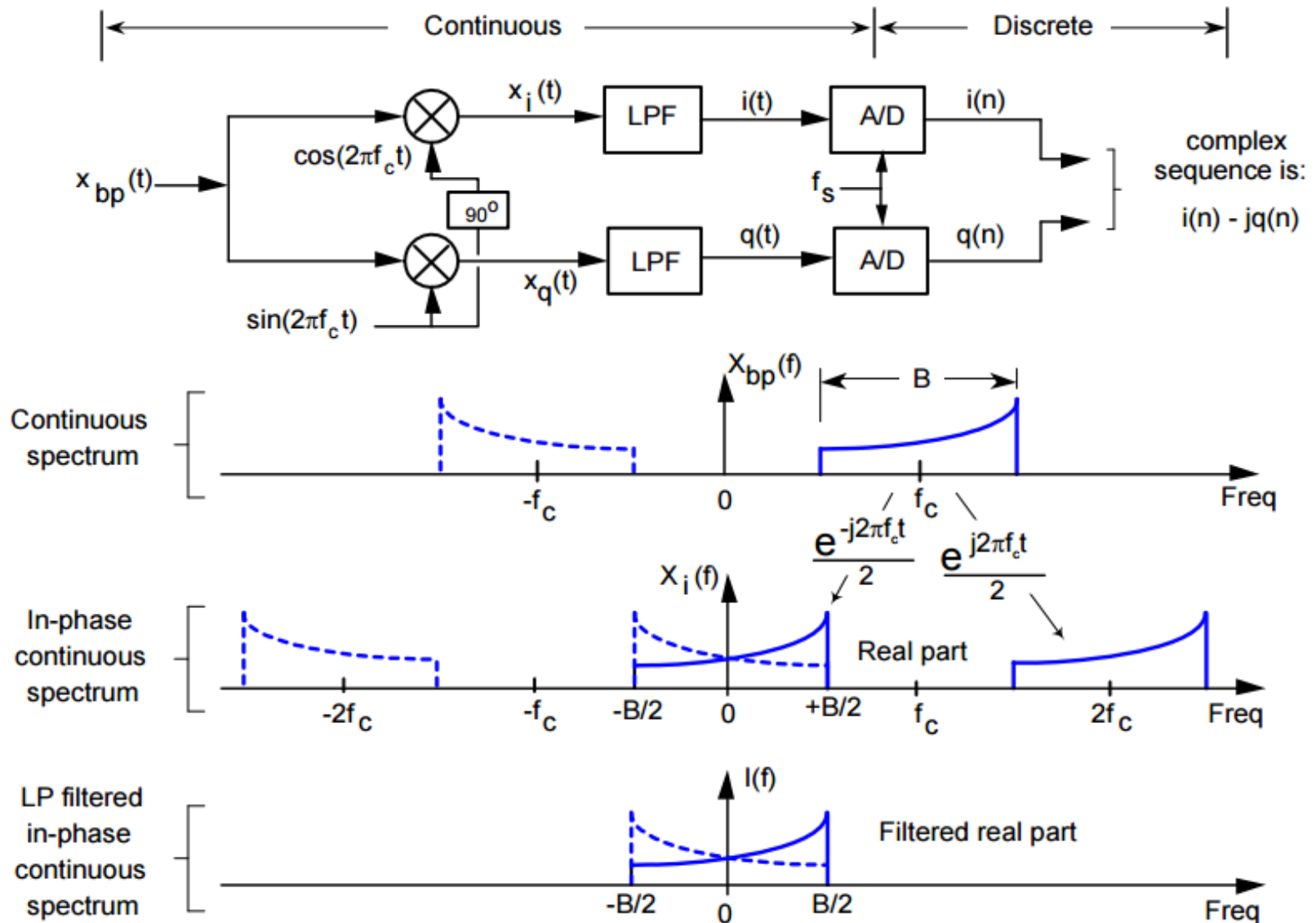
- Frequency range: 42 to 1002 MHz
- Noise figure : 3.5 dB @ RF_IN
- Phase noise: -98 dBc/Hz @ 10 kHz
- Current consumption: < 178 mA @ 3.3V power supply
- Max input power: +10 dBm
- Image rejection: 65 dBc

note: [dBm]=[dBuV on 75Ω] -108.75dB



THEORY OF RTL-SDR, I/Q RADIO

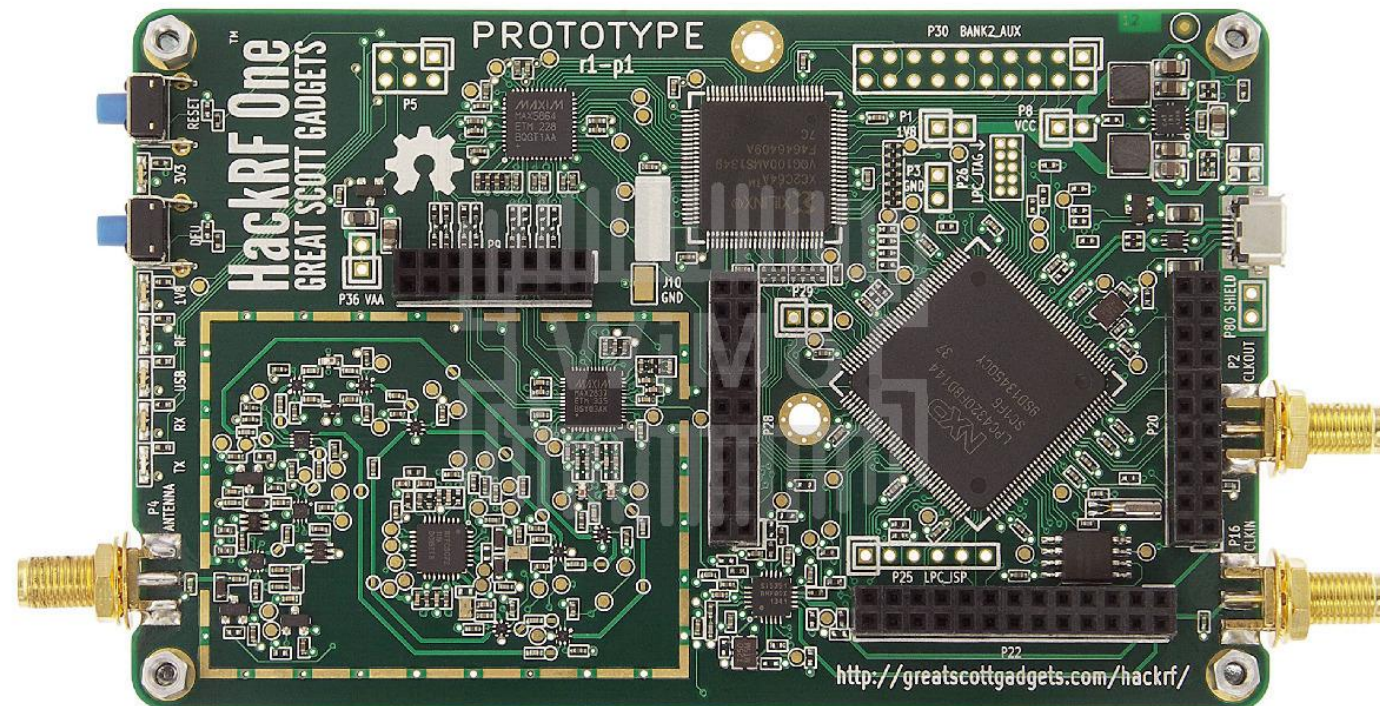
BASEBAND TO I & Q



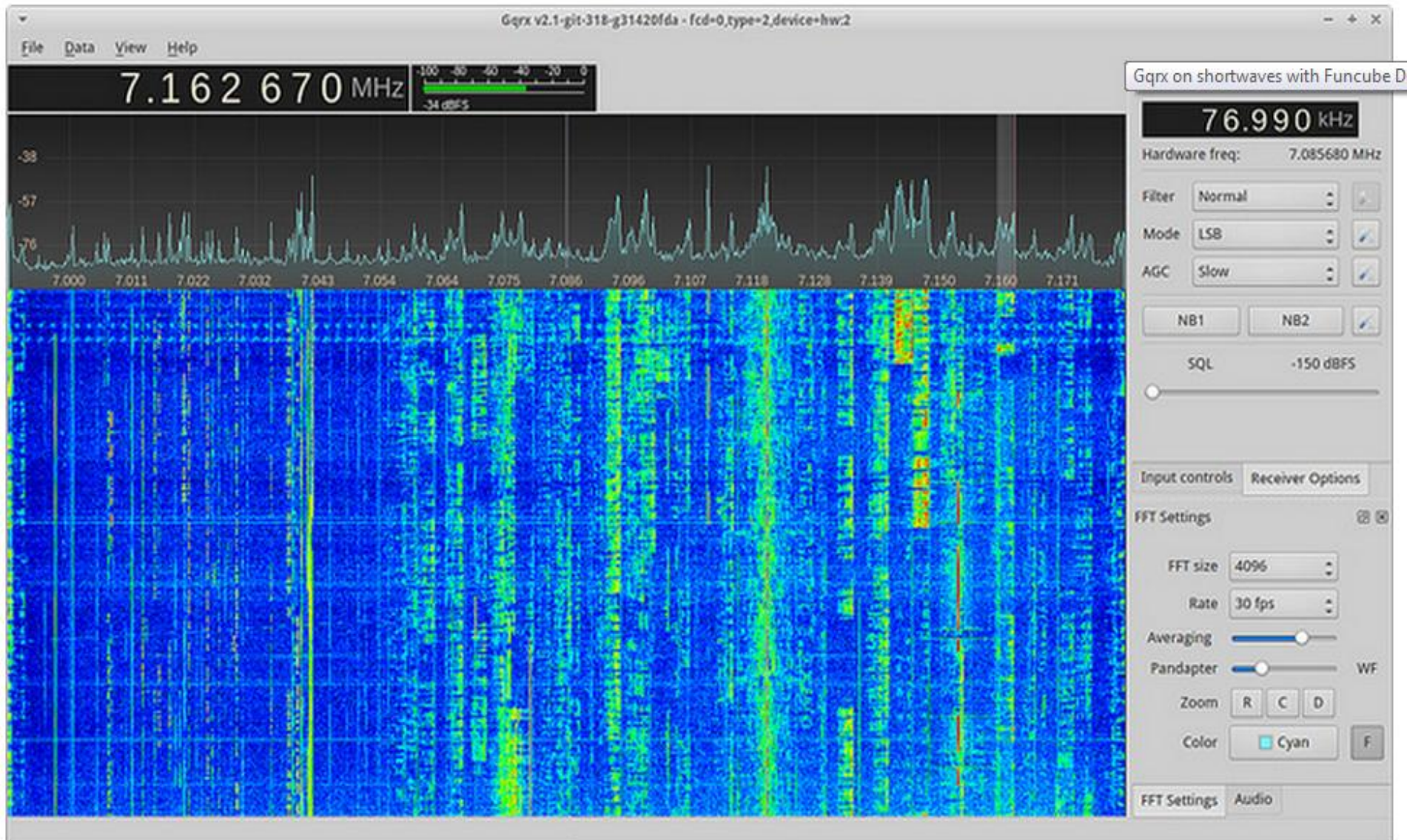
HACKRF, RX and TX SOFTWARE DEFINED RADIO

SPECIFICATIONS OF A LOW-COST TRANSMIT SDR

	HackRF
Radio Spectrum	30 MHz – 6 GHz
Bandwidth	20 MHz
Duplex	Half
Sample Size (ADC/DAC)	8 bit
Sample Rate (ADC/DAC)	20 Msps
Interface (Speed)	USB 2 HS (480 megabit)
FPGA Logic Elements	CPLD
Microcontroller	LPC43XX
Open Source	Everything
Availability	January 2014
Cost	\$300 [6]



LINUX SDR APPLICATION, GQRX



LINUX Based, Most Popular for Linux and available as LIVE Distribution USB (Boots into UBUNTU And Pre-installed GQRX)

SDR DIGITAL VOICE

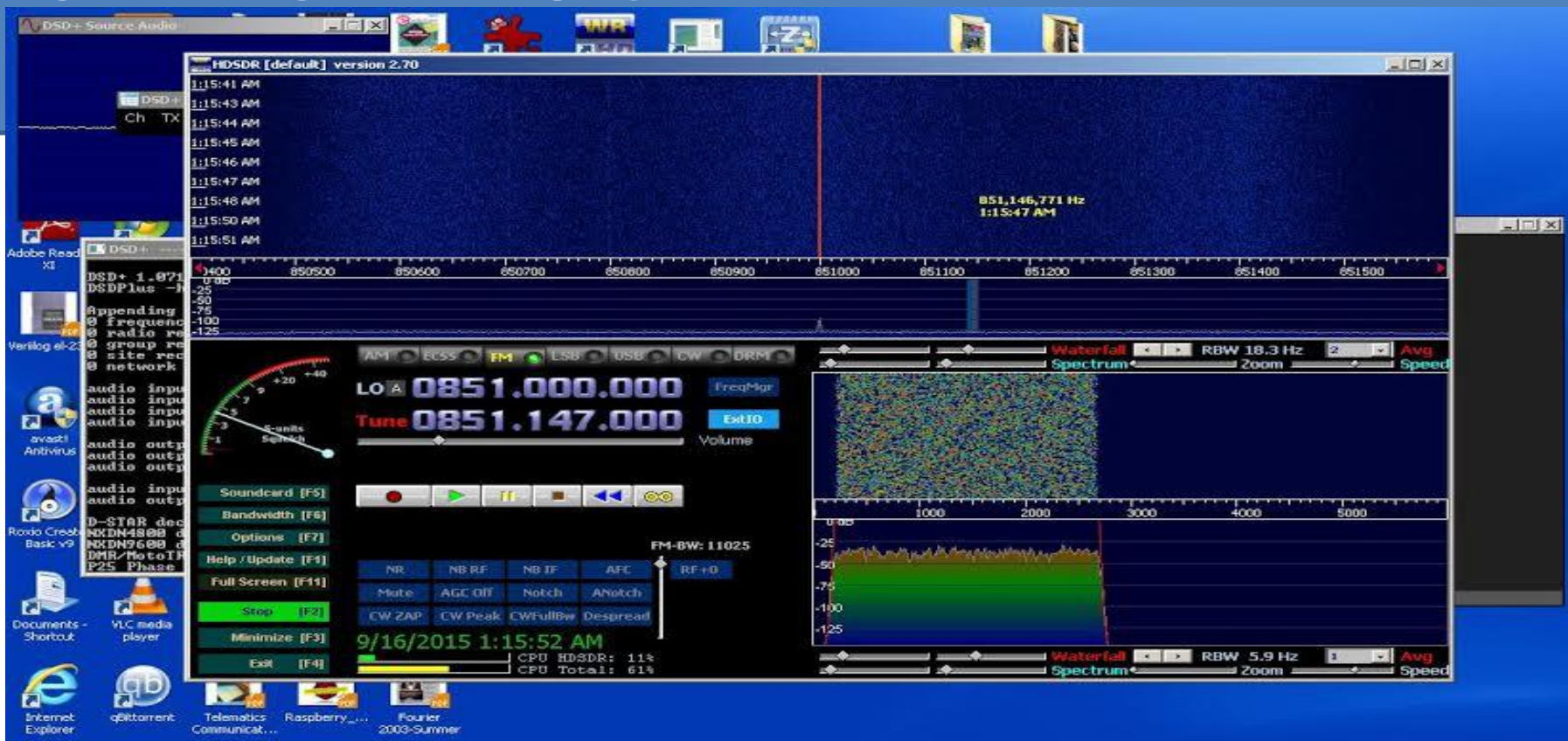
Digital Speech Codex such as P25 Phase 1, DMR/MOTOTRBO, Provoice, NXDN, and X2-TDMA

OVER A 24 HR PERSSION, ONLY 5% OF THE DATA TRAFFIC WAS ENCRYPTED!



DUAL TRUNKING RECEIVER <http://www.starsandstripes4sale.com/SDR-Radio.html>

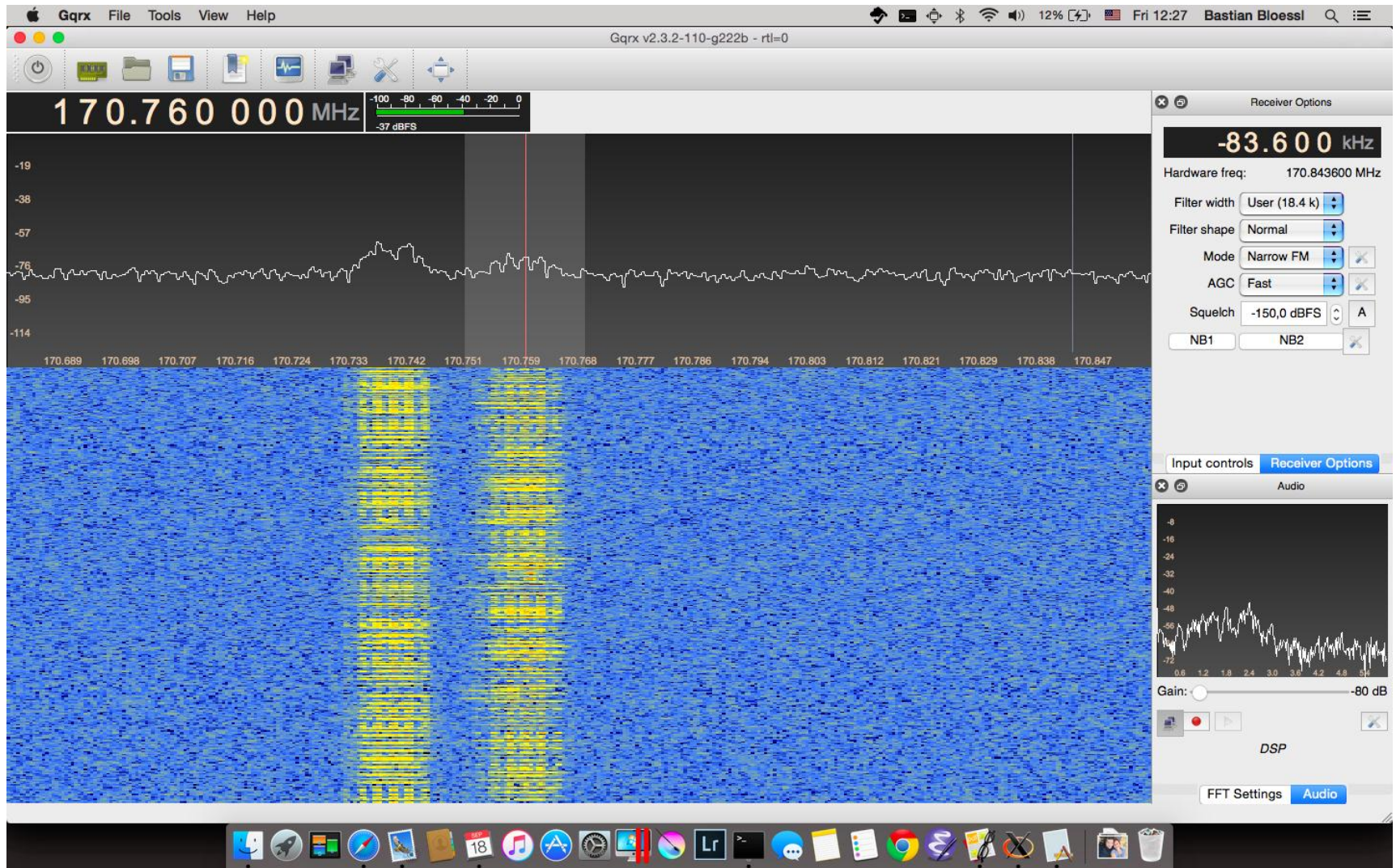
SDR DIGITAL VOICE



Frequency	License	Type	Tone	Alpha Tag	Description	Mode	Tag	
453.52500	WPTY620	RM	103.5 PL	HT PD 1	Police Dispatch		FMN	Law Dispatch
460.07500	KNCS282	RM	103.5 PL	HT PD 2	Police Operations		FMN	Law Talk
460.45000	KNCS282	RM	103.5 PL	HT PD 3	Police Operations		FMN	Law Talk
458.22500	WPTY620	BM		HT PD 4	Police Tactical / Special Events		FMN	Law Tac
155.38500	KEE600	M		HT EMS Tac	Municipal EMS Tactical		FMN	EMS-Tac
154.37000	KEG513	M	103.5 PL	HT FD Off.	Fire Officers	FMN	Fire-Talk	
154.22000	KED409	BM	103.5 PL	HT FD 4 FG	Fireground Operations		FMN	Fire-Tac
453.18750	WPIW453	M		HT DPW	Water & Sewer		FMN	Public Works

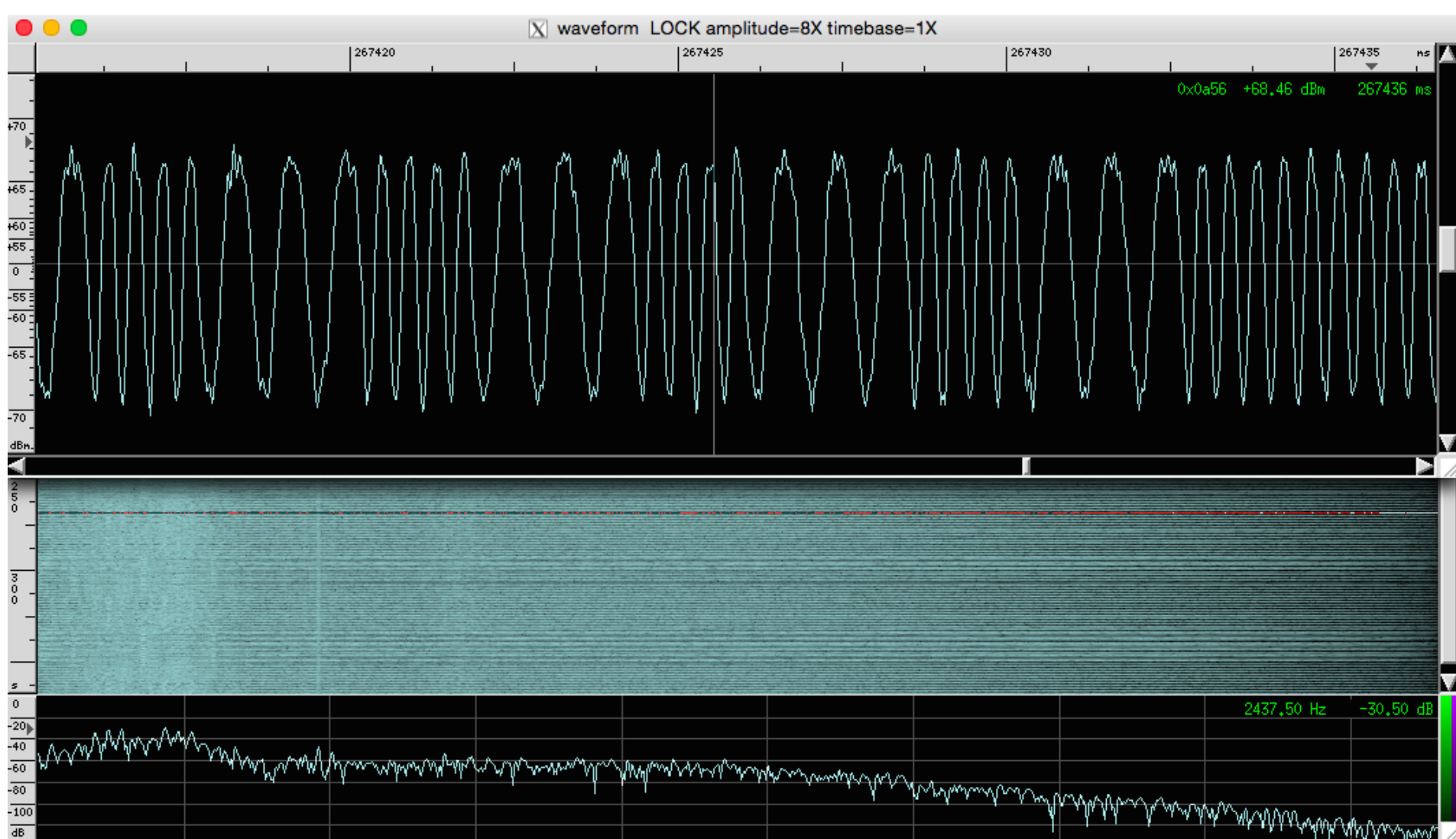
LOCAL TRANSMITTERS: <http://www.radioreference.com/apps/db/?ctid=1781>

SDR DEMODULATION and DECODING - Step 1



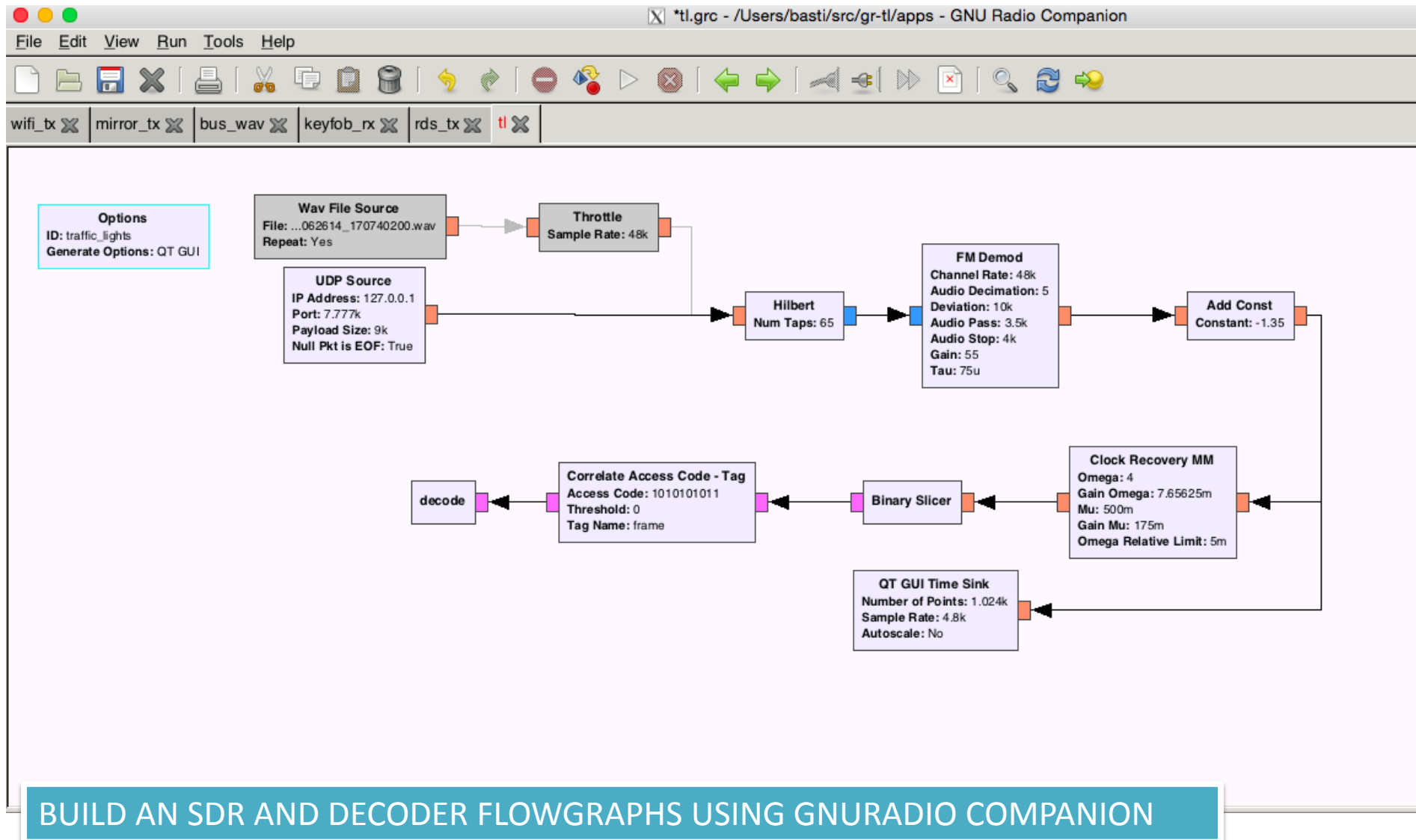
IDENTIFY THE CARRIER FREQUENCY and MODULATION

SDR DEMODULATION and DECODING - Step 2

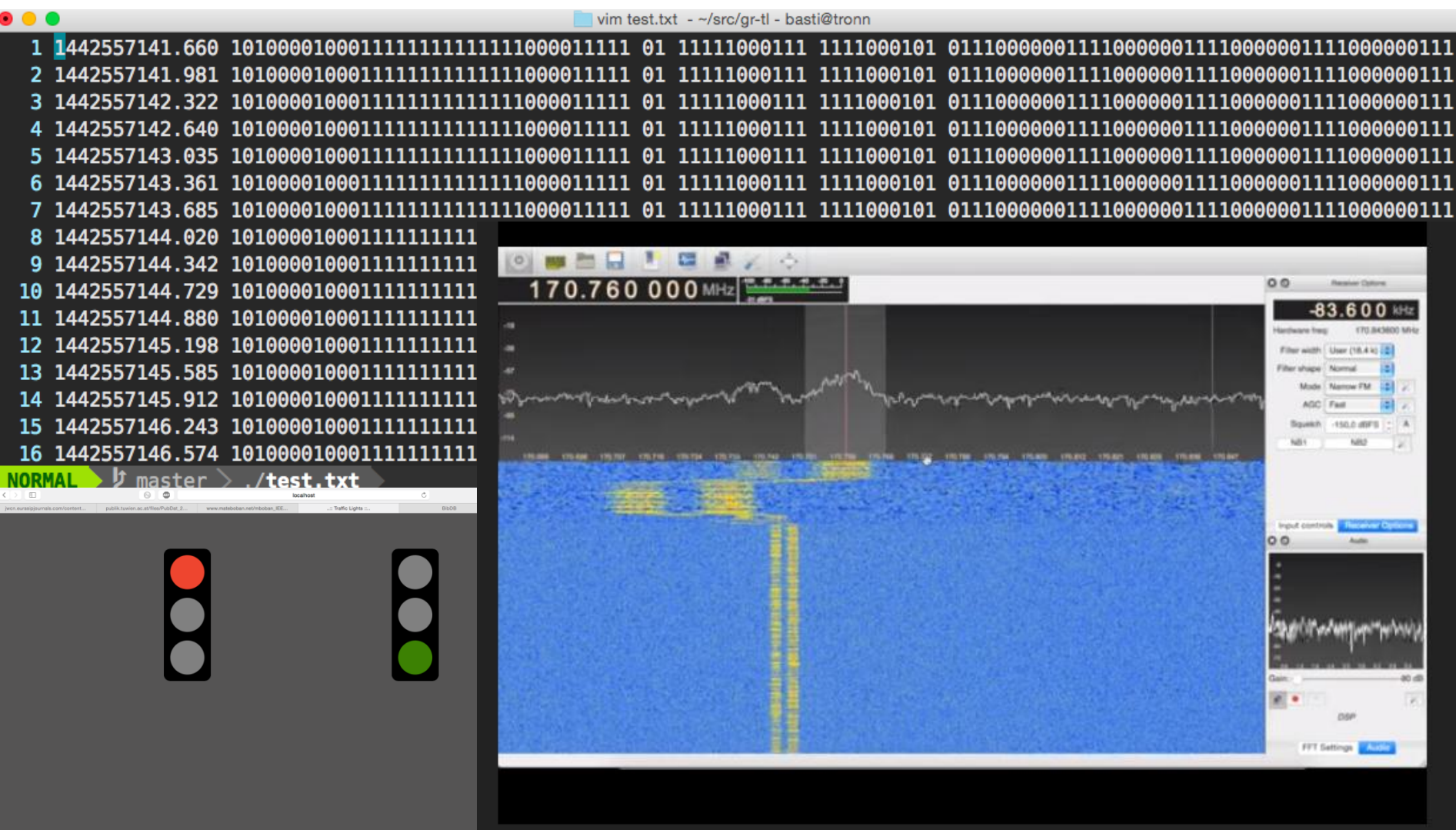


IDENTIFY THE DEMODULATED SIGNAL USING BAUDLINE OR AUDACITY

SDR DEMODULATION and DECODING - Step 3



SDR DEMODULATION and DECODING - Step 4



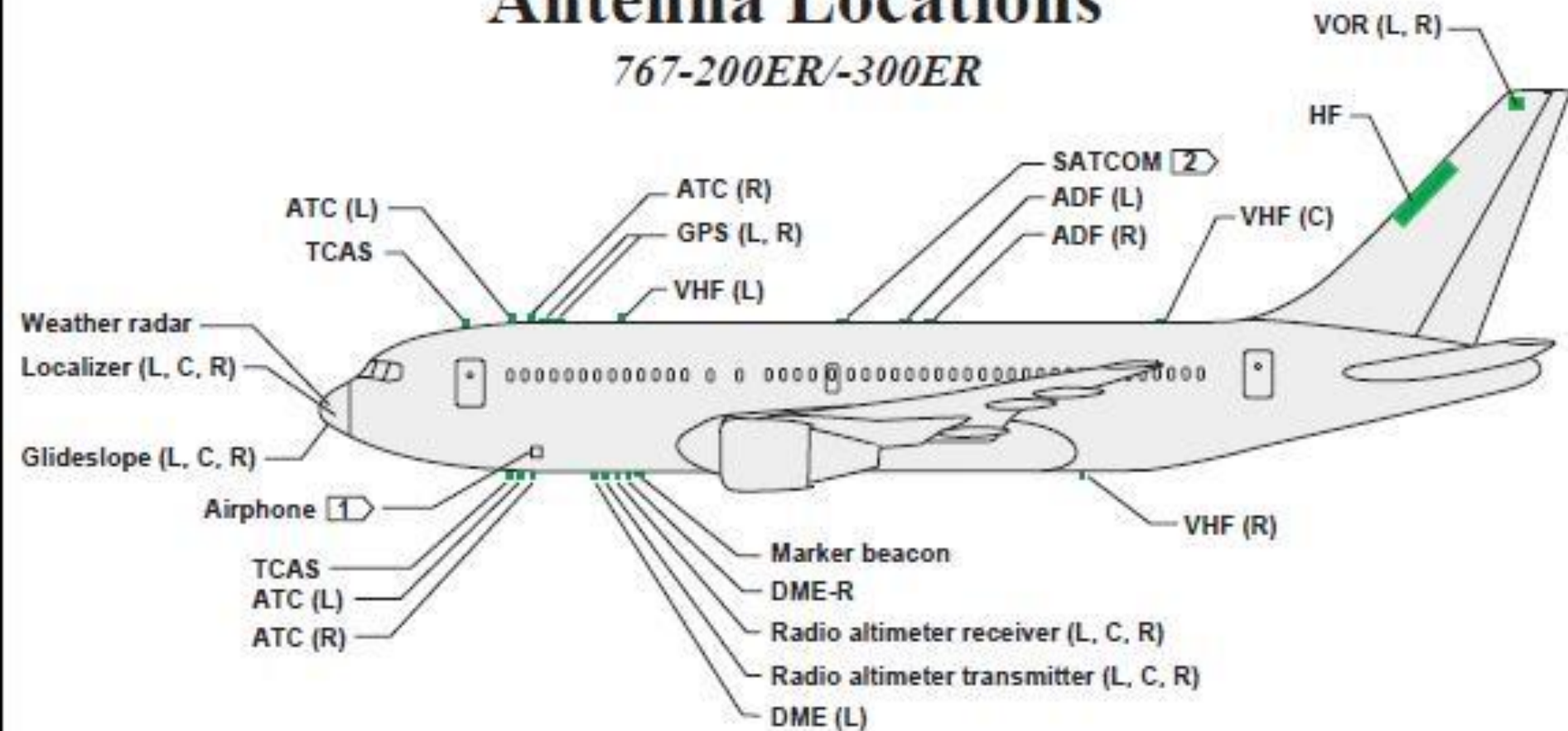
VIEW THE DATA SYNC PATTERN – WIRESHARK - AND MAP TO TRAFFIC LIGHTS!

<https://www.bastibl.net/page/3/>

RTL-SDR AIRCRAFT MONITORING

Antenna Locations

767-200ER/-300ER



AIRCRAFT ACARS

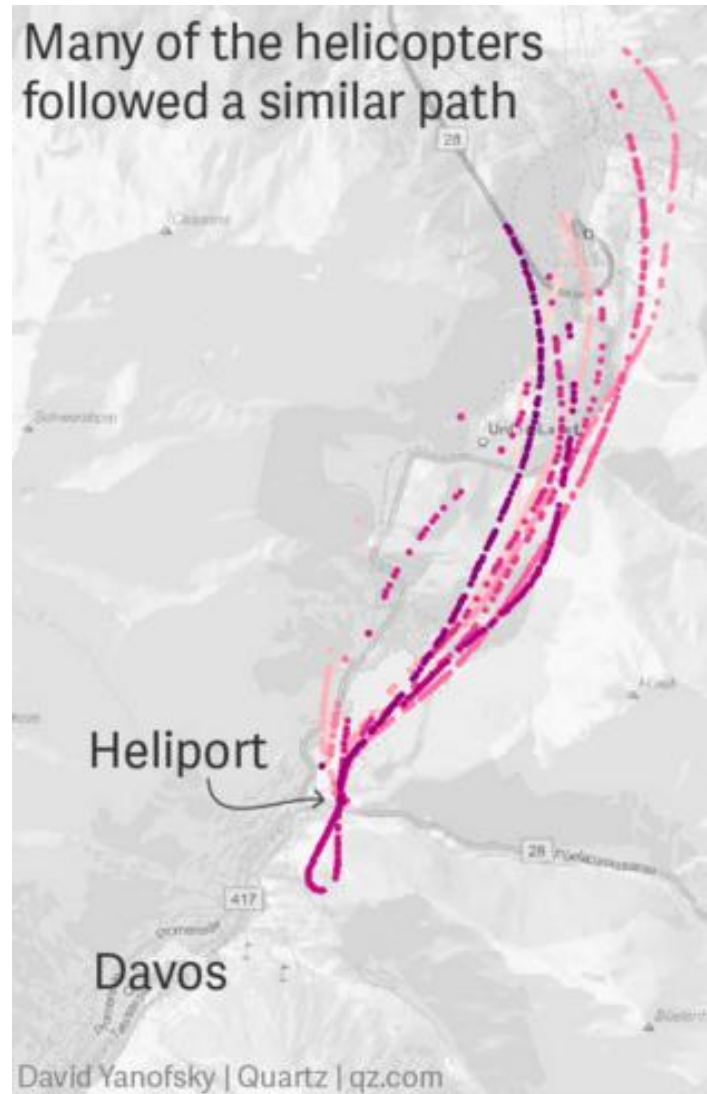
AIRCRAFT ACARS IS VHF, HF, AND SATELLITE

The screenshot displays the SDR software interface, which is divided into several sections:

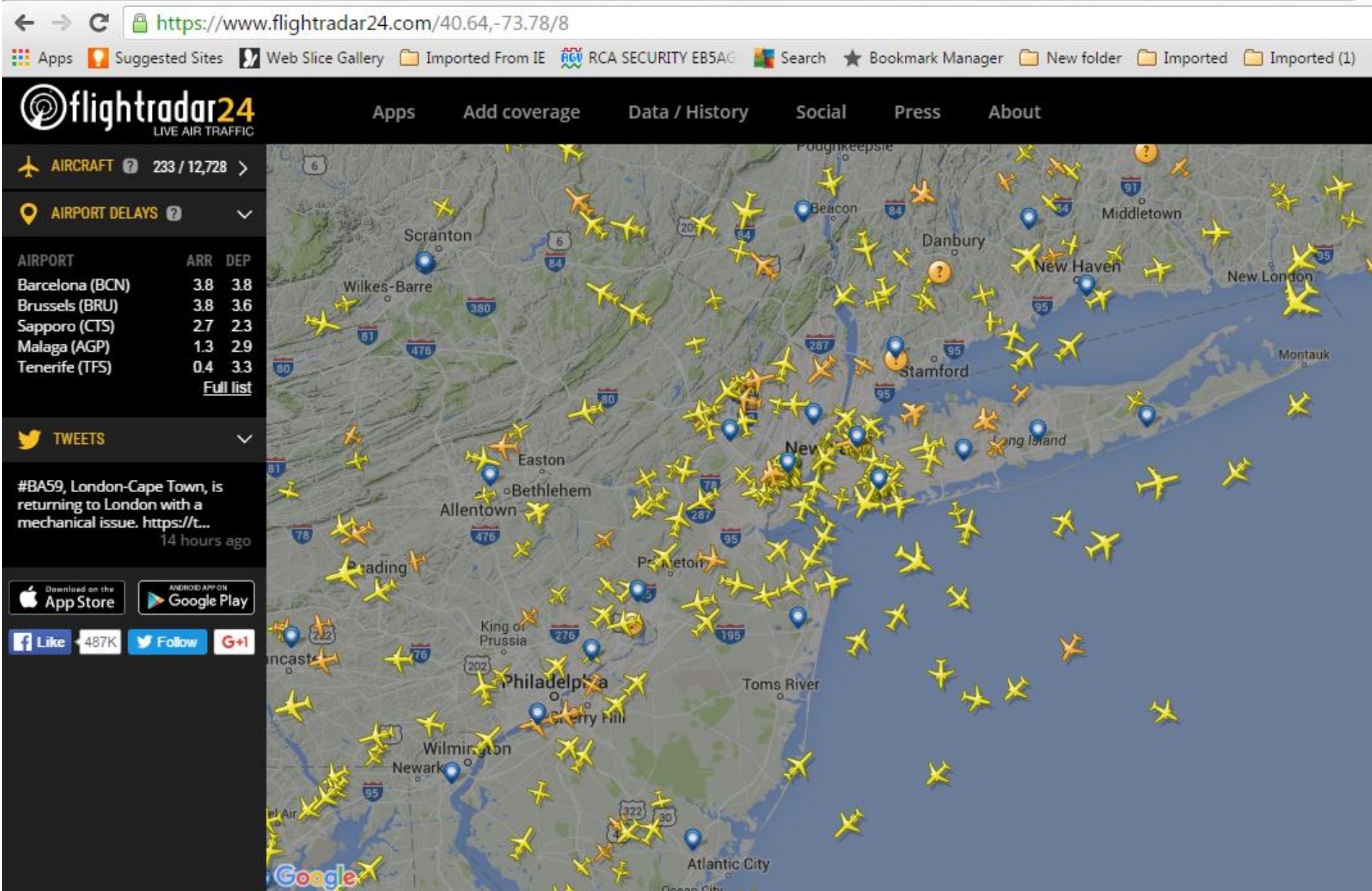
- Left Panel (Radio and Audio Controls):** Includes a 'Stop' button, a dropdown menu for 'RTL-SDR / USB', and a 'Configure' button. The 'Radio' section shows various modulation modes (NFM, AM, LSB, USB, WFM, DSB, CW, L, CWU) and a frequency display set to 131,739,153. The 'Audio' section includes an 'AF Gain' slider, a 'Sample rate' dropdown, and an 'Input' dropdown.
- Center Panel (Spectrum and Time):** Features a spectrum plot with a frequency range from 131,070 MHz to 131,740 MHz. Below the plot is a time display showing '12/10/2012 15:36:05'.
- Right Panel (ACARS Data and Aircraft Images):** Displays a list of ACARS messages with details such as 'ACARS mode', 'Aircraft reg', 'Message label', 'Block id', 'Msg no', and 'Flight id'. To the right of the messages are three small images of aircraft, labeled 'PZ-TCP', 'G-EUX', and 'LX-UCV'.
- Bottom Panel (Log and Status):** Contains a log of events, including '12 Oct 2012 - 15:31:57 Document contains no data' and '12 Oct 2012 - 15:34:53 Aircraft LX-UCV was added to your database'.

ADS-B AIRCRAFT AND HELICOPTER TRANSPONDERS

TRACKING THE WORLD ECONOMIC HEADQUARTERS' TRANSPORTATION HELICOPTERS @ 1090 MHz



UPLOADED AND SHARED ADS-B TRANSPONDERS



<https://www.flightradar24.com/40.64,-73.78/8>

AUTOMOTIVE SECURITY: OPEN “SECURE” DOORS [7]

DETERMINE KEY FOB FREQUENCY

Visualize Frequency and Modulation - FFT Waterfall

INTERFERE, OR JAM, BY TRANSMITTING ADJACENT SIGNAL

Interfere ~100 KHz below FOB Center Frequency

LISTEN AND CAPTURE CODE

Narrow the Receive Filter to Capture FOB Data Only

USER PRESSES KEY TWICE

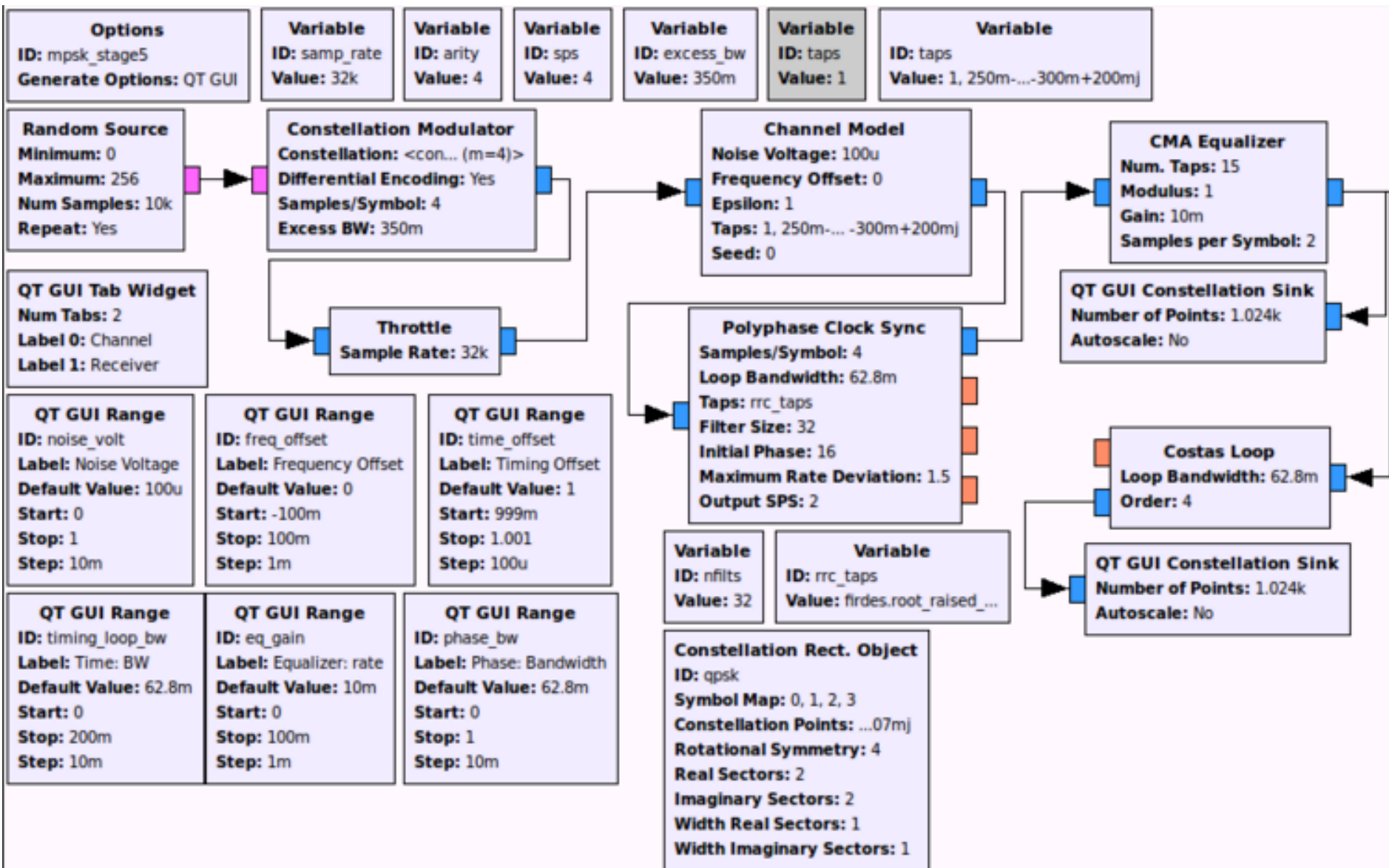
Unlock is being Prevented by Interfering Signal

RELAY CAPTURED CODES TO UNLOCK CAR

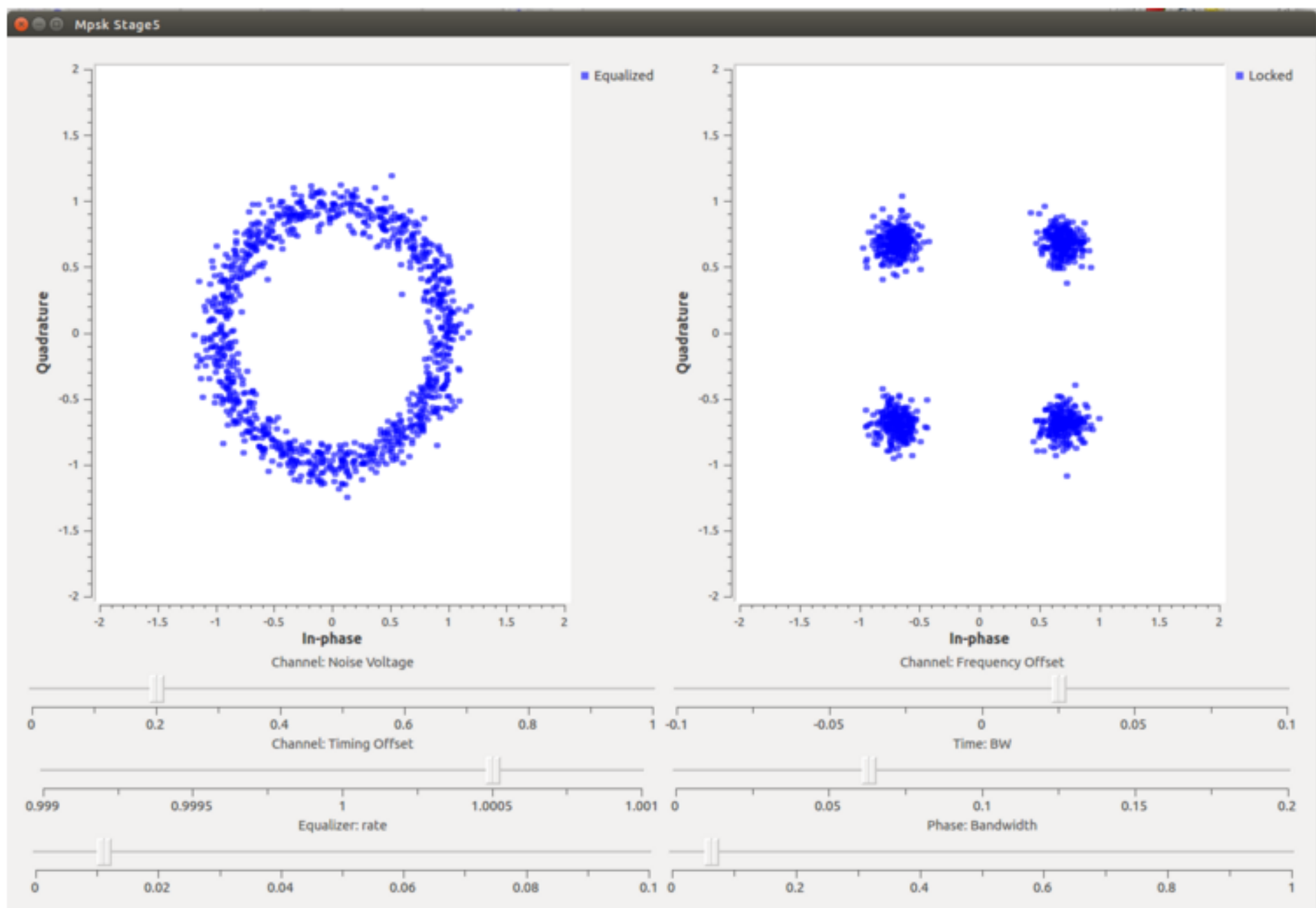
Two Codes Are Captured for Later Replay



SIGNALS ANALYSIS – WRITE FLOWGRAPHS IN GNURadio



COSTAS LOOP, LOCKED DATA CONSTELLATION



STINGRAY CELLULAR INTERCEPTION

\$400k BOX ACTS AS A BASE STATION (BTS) OR 2G TOWER

OPEN BTS UNIT ALSO WORKS WELL, APPLIED TO UNLOCKING SIMS



LOOKS LIKE A BTS (BASE STATION) TO A HANDSET

Handset is told to switch to 2G (RC5) if in LTE Region

<http://cloakers.org/stingray-cell-tower/>

iPHONE SECURITY - TEMPEST REVISITED

MONITORING PC/MAC/SMARTPHONE AT A DISTANCE

SENSE COHERENT RFI/EMI “NOISE” AND CORRELATE TO SCREEN INFORMATION



iPhone SECURITY

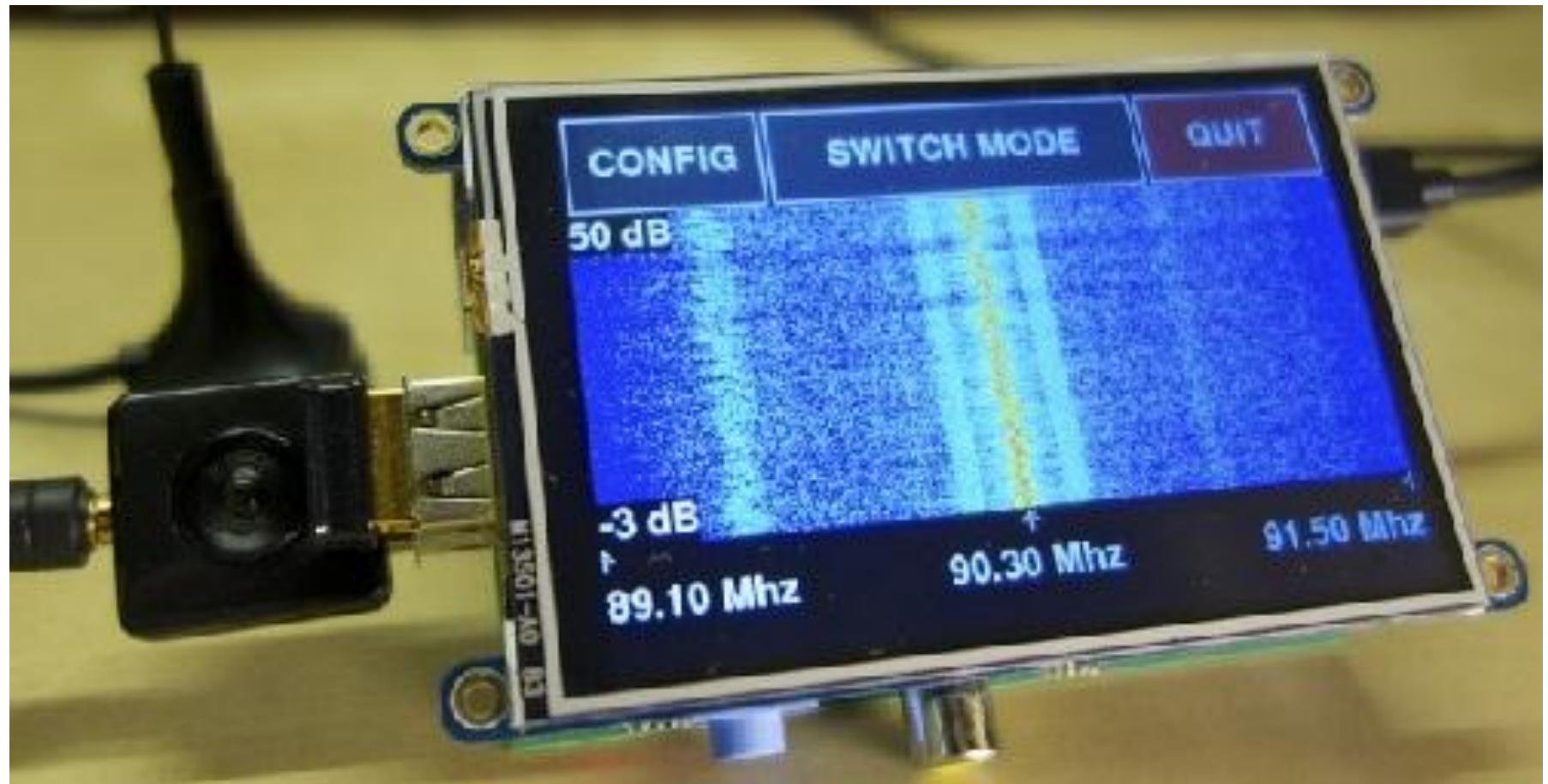
NOT WIRELESS: BRUTE FORCE USB-BASED PASSWORD TOOL

FBI's SUCCESSFUL METHOD AGAINST THE SAN BERNARDINO TERRORISTS' iPhone



<http://www.cellebrite.com/>

RLT-SDR + RasPI2 Experimenters Delight [8]



WIRELESS SECURITY CONCLUSIONS

WIRELESS STANDARDS LIMIT INTERNET-OF-THINGS GROWTH

- ✓ **EXISTING WIRELESS STANDARDS ARE NOT SECURE**
- ✓ **MINIMAL WL ENCRYPTION STANDARD – TODAY - IS AES256**
- ✓ **AIRPLANE ACARS AND TRANSPONDER WIRELESS SYSTEMS CAN BE COMPROMISED AND SPOOFED**
- ✓ **GSM RC5 ENCRYPTION STANDARDS ARE COMPROMISED**
- ✓ **MOST POLICE DIGITIZED VOICE TRAFFIC IS IN THE CLEAR**
- ✓ **FUTURE IoT IMPLEMENTATIONS REQUIRE IMPROVED ENCRYPTION STANDARDS**

REFERENCES

- [1] Edward Kujawski, "The Boat Anchors Manual Archive : /rca/ar88"
<http://bama.edebris.com/manuals/rca/ar88/>
- [2] Henry Rogers, "RCA's Amazing AR-88 Receivers" <http://www.radioblvd.com/ar88.htm>
- [3] Fred Osterman, *et al.*,
"Shortwave Receivers Past & Present: Communications receivers 1942-2013," Fourth Edition,
Universal Radio Research, pp. 569 - 578, Aug. 2015
- [4] Robert W Stewart, Kenneth W Barlee , Dale S W Atkinson, *et al.*,
"Software Defined Radio using MATLAB & Simulink and the RTL-SDR," Strathclyde Press, 2015
- [5] Robert W Stewart, Kenneth W Barlee , Dale S W Atkinson, *et al.*, "Software Defined Radio
using MATLAB & Simulink and the RTL-SDR," PDF VERSION, <http://www.desktopsdr.com/>
- [6] Big List of RTL-SDR Applications Software: <http://www.rtl-sdr.com/big-list-rtl-sdr-supported-software/>
- [7] Samy Kamkar, "DEFCON Drive it liked you Hacked it", Defcon 23, 2015
<http://samy.pl/defcon2015/>
- [8] Adafruit : <https://learn.adafruit.com/freq-show-raspberry-pi-rtl-sdr-scanner/overview>