

Fun With Satellites

Stories regarding a bunch of noobs that try to:

- **MAKE** a robotic UHF satellite tracking station (SatNOGS - work in progress :-)
- “**HACK**” Inmarsat STD-C EGC Messages (public shipping broadcast comms)
- **VOID** a GPS antenna’s warranty quite badly to listen to non-GPS satellites



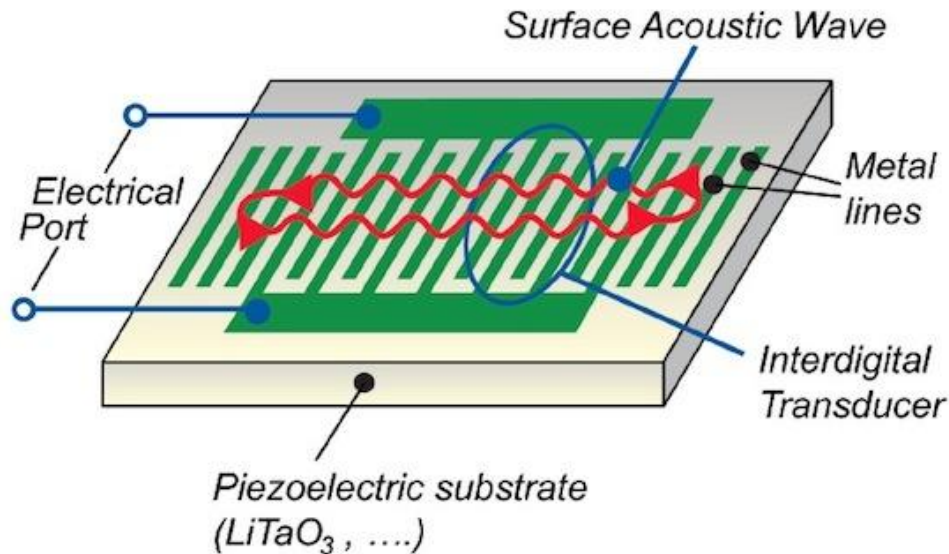
MAKE. HACK. VOID

A Canberra Hackerspace

L-Band & cheap GPS antennas

- L-Band: 1-2GHz
- GPS frequency is 1575.42MHz
- SAW filters are cool¹:
- What can we receive?

www.uhf-satcom.com/lband/



1: <http://www.edn.com/design/wireless-networking/4413442/SAW--BAW-and-the-future-of-wireless>

L-Band satellite frequencies (some of them!)

Position	Freq	Service / Modulation / Notes
98.14W	1525.870	BGAN 33.6 40kHz ACF=80.2ms
Inmarsat 4F3	1528.785	LES 360 Local=0 Joint NCS+TDM - private LES TDMA BPSK 1200bps
(tnx to blh,)	1528.805	LES 360 Local=1 Joint NCS+TDM - private LES TDMA BPSK 1200bps
(trango and)	1530.953	6Kbps BPSK weak
(root)	1531.240	BGAN ~100kHz weak
	1531.710	LES 056 Local=2 Joint NCS+TDM - private LES TDMA BPSK 1200bps
	1531.750	LES 253 Local=1 Joint NCS+TDM - private LES TDMA BPSK 1200bps
	1531.770	LES 254 Local=1 Joint NCS+TDM - private LES TDMA BPSK 1200bps
	1531.790	LES 252 Local=1 Joint NCS+TDM - private LES TDMA BPSK 1200bps
	1531.810	LES 054 Local=3 Joint NCS+TDM - private LES TDMA BPSK 1200bps
	1532.080	BGAN ~100kHz weak
	1533.215	LES 361 Local=0 Joint NCS+TDM - private LES TDMA BPSK 1200bps
	1533.285	LES 361 Local=1 Joint NCS+TDM - private LES TDMA BPSK 1200bps
	1533.615	6Kbps BPSK? weak
	1533.625	Std-B NCS
	1533.635	Std-M LES 0xBD
	1535.1375	Seastar DGPS point to multipoint BPSK 2438bps {id=0xC685 scr=0x5C08}
	1535.175	Veripos DGPS correction data BPSK 2438bps (High Power) {id=???? scr=0x1D2F}
	1536.900	BGAN ~160khz
	1537.0625	BGAN 8400bps QPSK
	1540.300	BGAN ~160khz
	1542.500	BGAN ~160khz
	1542.700	BGAN ~160khz
	1543.140	LES 252 Local=0 Joint NCS+TDM - private LES TDMA BPSK 1200bps
	1543.160	LES 253 Local=0 Joint NCS+TDM - private LES TDMA BPSK 1200bps
	1543.180	LES 054 Local=0 Joint NCS+TDM - private LES TDMA BPSK 1200bps
	1543.185	BPSK 2498Bd 2240bit frame
	1543.205	LES 051 Local=0 Joint NCS+TDM - private LES TDMA BPSK 1200bps
	1543.250	LES 056 Local=0 Joint NCS+TDM - private LES TDMA BPSK 1200bps
	1543.290	2400bps BPSK BURSTS
	1543.305	LES 053 Local=1 Joint NCS+TDM - private LES TDMA BPSK 1200bps
	1543.310	3372bps QPSK - Inmarsat AMSC LES
	1543.350	LES 254 Local=3 Joint NCS+TDM - private LES TDMA BPSK 1200bps
	1543.379	2400bps BPSK BURSTS
	1543.380	LES 052 Local=2 Joint NCS+TDM - private LES TDMA BPSK 1200bps
	1543.395	LES 054 Local=1 Joint NCS+TDM - private LES TDMA BPSK 1200bps
	1543.955	BPSK 2498Bd 2240bit frame
	1545.545	SkyFire DGPS 1200BPSK
	1546.840	3372bps QPSK - Inmarsat AMSC LES

<http://www.uhf-satcom.com/lband/>

Inmarsat AERO messages

The screenshot shows the JAERO software interface. At the top, there is a menu bar with 'File', 'Tools', and 'Help'. Below the menu bar are several icons representing different functions. The main display area is divided into three sections:

- Message List:** A list of five received messages, each with a header and a body. The headers are: 1 0x0A 0x57 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00, 2 0x26 0x01 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00, 3 0x0A 0x57 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00, 4 0x26 0x01 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00, and 5 0x0A 0x57 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00. The bodies are: rec = A20A calc = A20A OK AES_system_table_broadcast_index, rec = 6AE2 calc = 6AE2 OK Reserved_26, rec = A20A calc = A20A OK AES_system_table_broadcast_index, rec = 6AE2 calc = 6AE2 OK Reserved_26, and rec = A20A calc = A20A OK AES_system_table_broadcast_index.
- Message Header:** 12:38p.m. Mon 7-Dec-2015 JAERO started
- Message Body:** 12:39:50 07-12-15 AES:71BF43 GES:82 2 .HL7743 ! A9 K
SELATYA.TI2/RKSI ARR ATIS X
2330Z
EXP ILS APCH RWY 33R
WIND 040/6KT
CAVOK
T MS 2 DP MS 8
QNH 1031
FLOCKS OF BIRDS VICINITY AIRPORT USE CAUTION
2266

At the bottom of the interface, there is a signal spectrum plot showing a blue signal waveform over a frequency range from 800 to 5600 Hz. A green shaded region highlights the signal between approximately 800 and 1600 Hz. To the right of the plot is a constellation diagram showing a grid of yellow dots. Below the plot are three status indicators: Volume (green circle), Signal (green circle), and Data (green circle). At the bottom right, there are several control buttons: Speed (600 bps), Locking (900 Hz), AFC on, Display, and Constellation. The bottom status bar shows Freq: 1133.17Hz and EbNo: 15dB.

Inmarsat STD-C EGC MESSAGES messages

Military Operations: Live Firing Warning

STRATOS CSAT 4-AUG-2015 03:21:25 436322 SECURITE FM: RCC NEW ZEALAND 040300 UTC AUG 15
COASTAL NAVIGATION WARNING 151/15 AREA COLVILLE, PLENTY CUVIER ISLAND (REPUNGA ISLAND),
BAY OF PLENTY 1. LIVE FIRING 060300 UTC TO 060500 UTC AUG 15 IN DANGER AREA NZM204. ANNUAL
NEW ZEALAND NOTICES TO MARINERS NUMBER 5 REFERS. 2. CANCEL THIS MESSAGE 060600 UTC AUG 15
NNNN

Armed Robbery / Pirate Warning

NAVAREA XI WARNING NAVAREA XI 0571/15 SINGAPORE STRAIT. ARMED ROBBERY INFORMATION.
301845Z JUL. 01-04.5N 103-41.8E. FIVE ROBBERS ARMED WITH LONG KNIVES IN A SMALL UNLIT HIGH
SPEED BOAT APPROACHED A BULK CARRIER UNDERWAY. ONE OF THE ROBBERS ATTEMPTED TO BOARD
THE SHIP USING A HOOK ATTACHED TO A ROPE. ALERT CREW NOTICED THE ROBBER AND RAISED THE
ALARM AND CREW RUSHED TO THE LOCATION. HEARING THE ALARM AND SEEING THE CREW ALERTNESS,
THE ROBBERS ABORTED THE ATTEMPTED ATTACK AND MOVED AWAY. INCIDENT REPORTED TO VTIS
SINGAPORE. ON ARRIVAL AT SINGAPORE WATERS, THE COAST GUARD BOARDED THE SHIP FOR
INVESTIGATION. VESSELS REQUESTED TO BE CAUTION ADVISED.

<http://www.rtl-sdr.com/rtl-sdr-tutorial-decoding-inmarsat-std-c-egc-messages/>

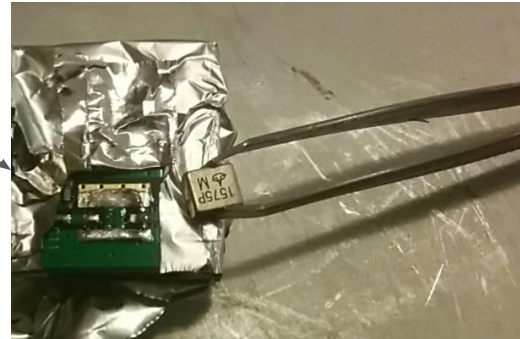
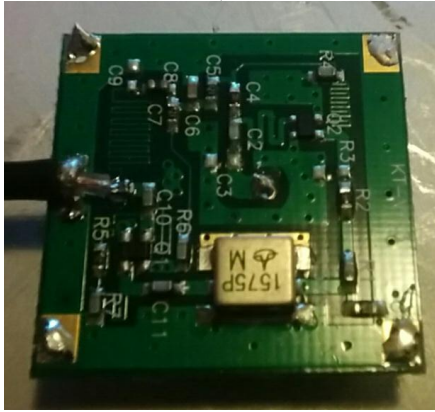
Iridium pager traffic

Sub-type 2: SMS

- 09.01 contains SMS
- Tested with leased Iridium phone: Iridium 9555

```
0901 8f.01.01.07.91.88.61.26.09.00.50.00.83.24.0e.80.00.88
.61.26.99.00.00.20.00.51.01.51.91.73.12.00.7e.c4.b2.1c.a4.ad
.9f.c3.ee.33.48.5f.07.0d.df.6d.78.9d.5e.96.bb.41.75.37.19.14
.66.b3.cb.6d.16.e8.1e.9e.83.ca.69.77.b9.0d.d2.97.d3.e7.b2.1b
.b4.0e.bb.dd.2c.d0.3d.5d.06.91.d3.e5.79.19.74.2d.b3.e9.20.73
.dd.bd.a6.a7.df.ee.74.59.4e.67.81.e6.6f.36.9b.5e.06.d5.dd.e2
.f2.59.5e.76.eb.e9.a0.ba.9b.0c.b2.bf.d9.ec.39.7d.ef.26.a7.cf
.a0.79.39.ed.76.01.00.00.00.00.00.00.00.00.00.00.00.00.00
```

GPS Antenna Mod



Volume

Quality

SYNC Lost Packets #

CRC

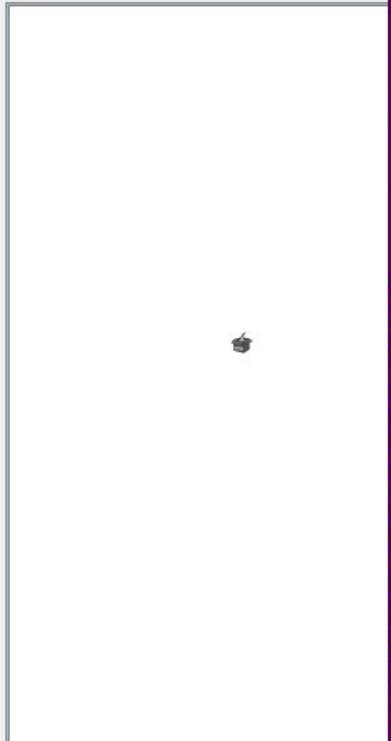
1900

Cent

Acc

Dete

Terminal

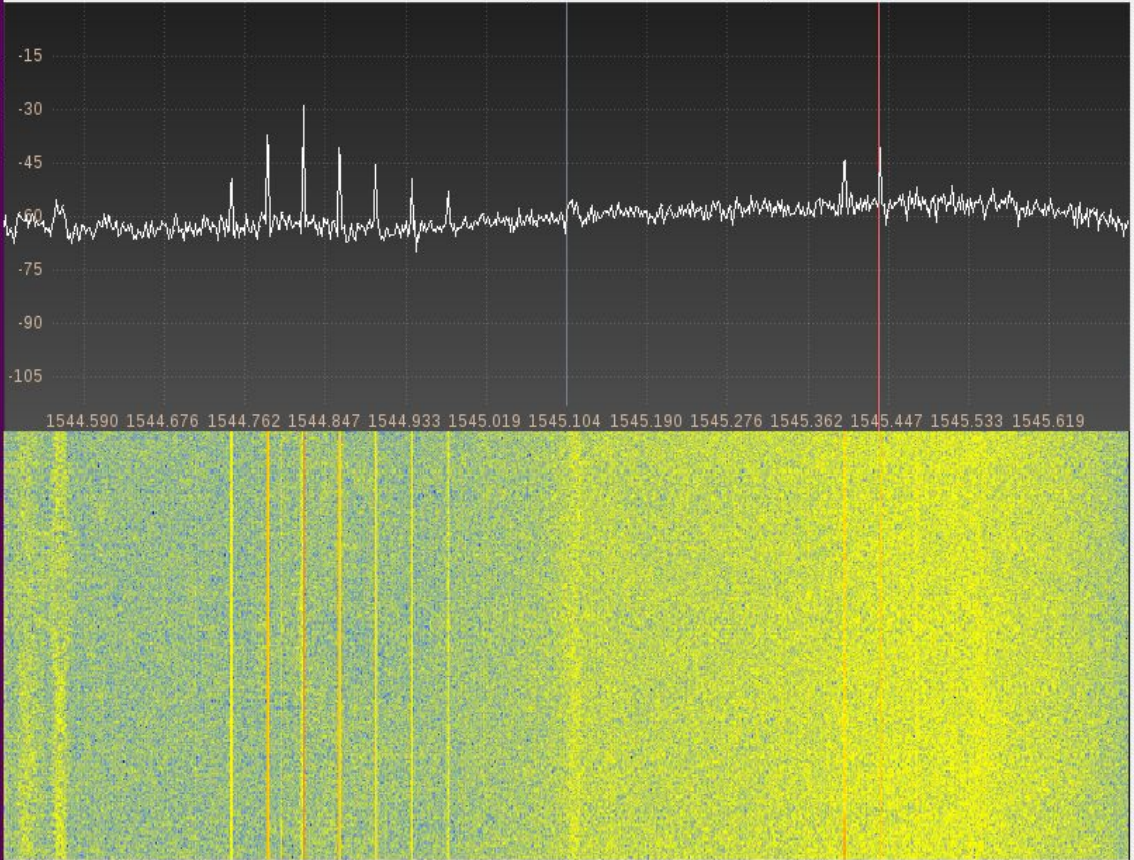


File Tools View Help

1,545.436 270 MHz

-100 -80 -60 -40 -20 0

-31 dBFS



Receiver Options

331.850 kHz

Hardware freq: 28.504420 MHz

Filter Normal

Mode USB

AGC Fast

Squelch -150.0 dBFS

NB1 NB2

Input controls Receiver Options

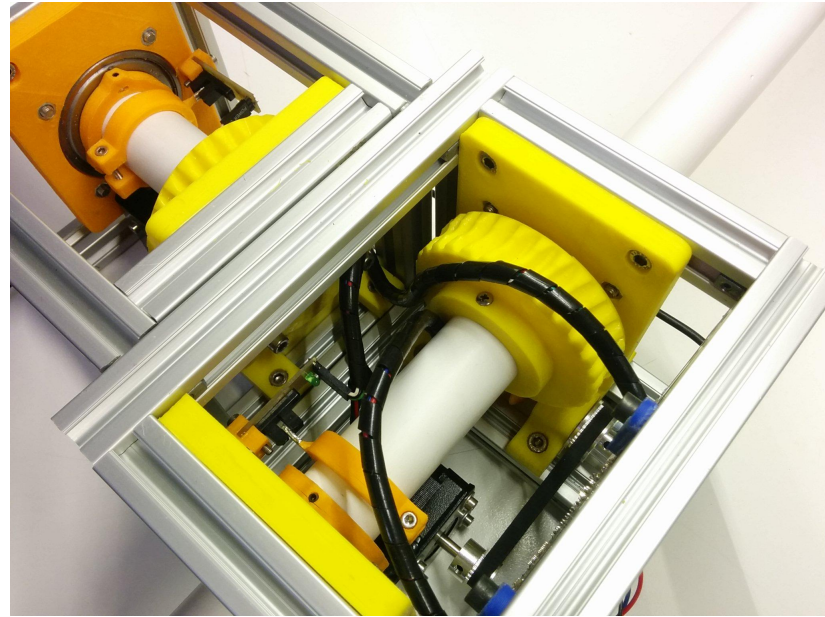
Audio

Gain: 3.4 dB

DSP

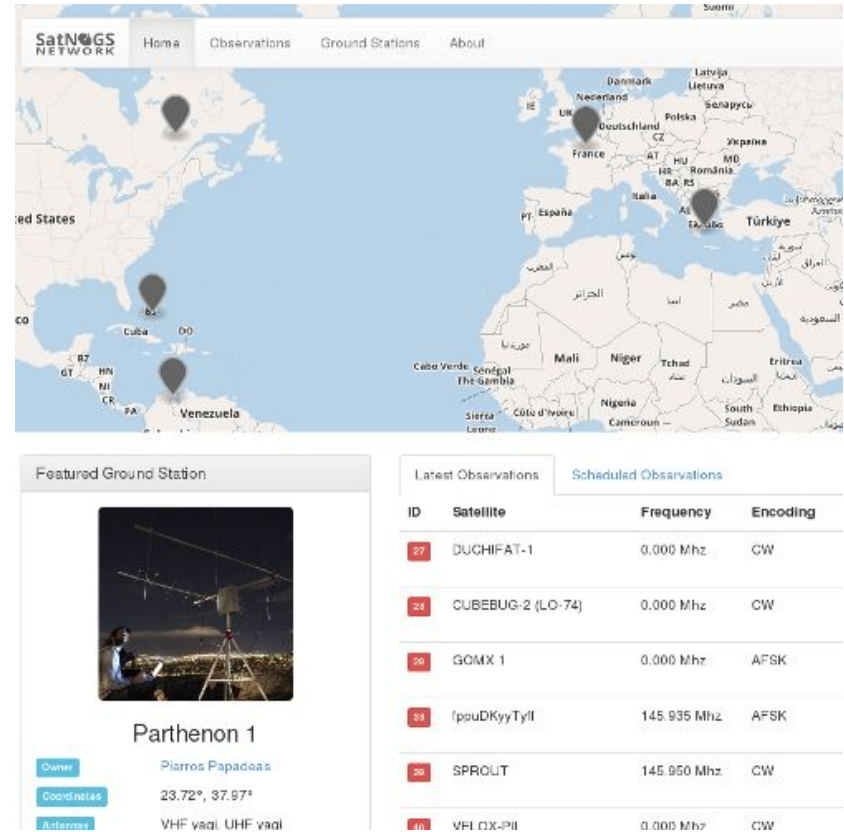
FFT Settings Audio

SatNOGS! - <https://satnogs.org/>



<https://satnogs.org/documentation/hardware/>

SatNOGS network

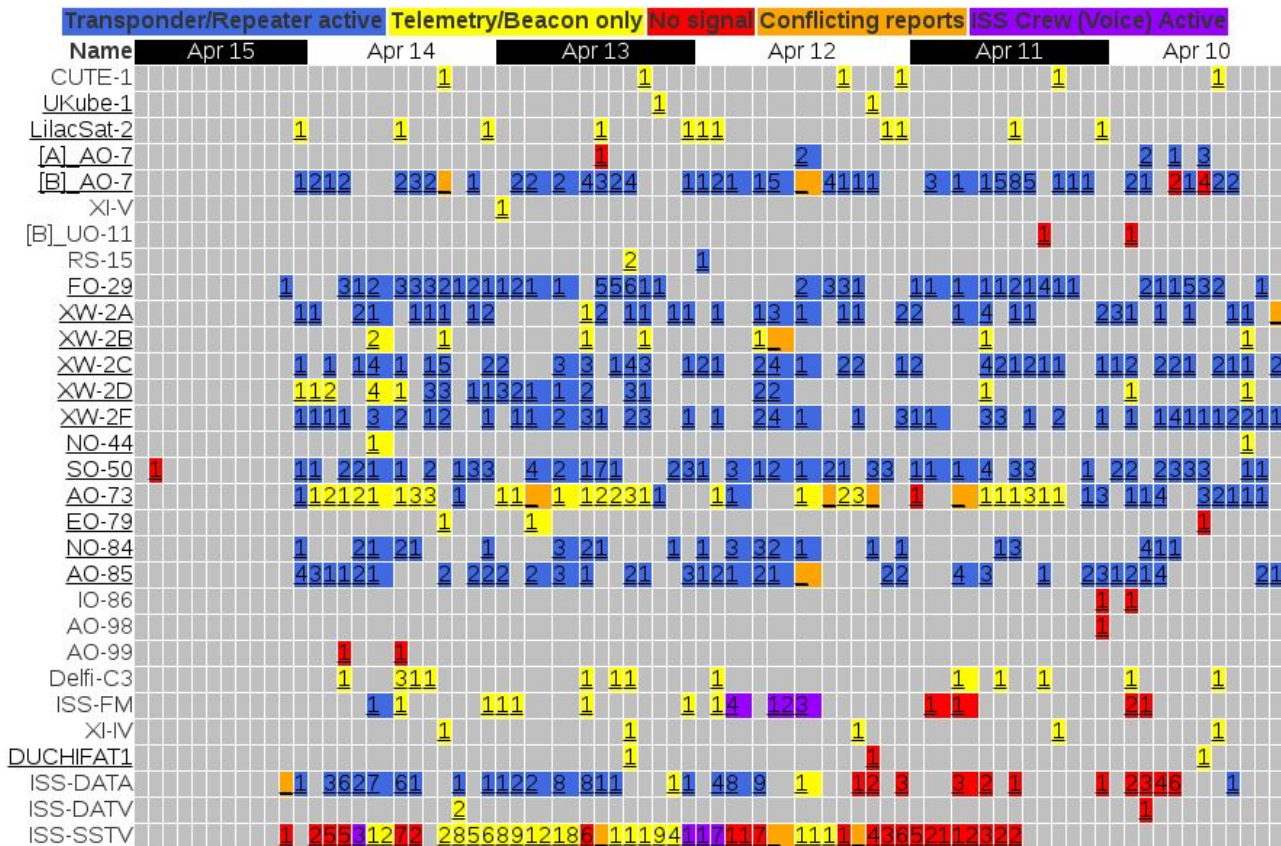


The screenshot shows the SatNOGS Network website. At the top, there is a navigation menu with 'Home', 'Observations', 'Ground Stations', and 'About'. Below the menu is a world map with several ground station locations marked by black pins. The 'Featured Ground Station' section displays a photo of the 'Parthenon 1' station at night, with a person operating it. Below the photo, the station's details are listed: Owner (Piarros Papadonas), Coordinates (23.72°, 37.97°), and Antennas (VHF vadi, UHF vadi). To the right, there are two tabs: 'Latest Observations' and 'Scheduled Observations'. The 'Latest Observations' tab is active, showing a table of recent observations.

ID	Satellite	Frequency	Encoding
27	DUCHIFAT-1	0.000 Mhz	CW
28	CUBEBUG-2 (LO-74)	0.000 Mhz	CW
29	GOMX 1	0.000 Mhz	AFSK
38	!pouDKyyTyll	145.935 Mhz	AFSK
39	SPROUT	145.950 Mhz	CW
46	VFL OX-Pil	0.000 Mhz	CW

<https://satnogs.org/>

Amateur Satellites



<http://amsat.org/status/>

Hackerspaces are awesome

- 3D Prints from Monika, Paul.B, Max, Ian, Iggy, Steve
- Mechanical assembly from Declan, Joseph
- Testing adventures with Adam, Jamie, Ian, Paul.B, Declan, Max



MAKE. HACK. VOID

A Canberra Hackerspace

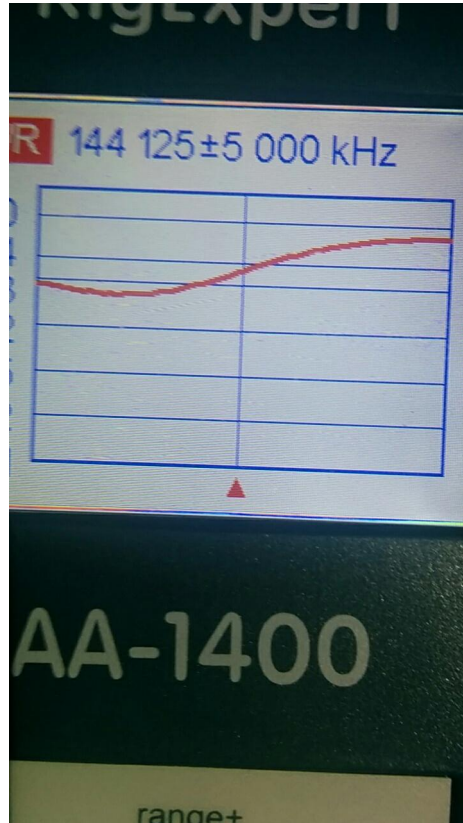
Testing adventures



Junk yard wars VHF Yagi



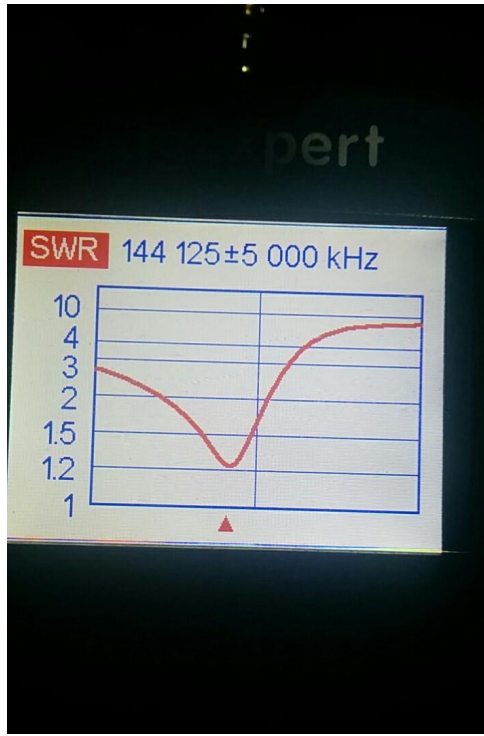
But we haven't attempted any impedance matching!



Enter the “Buckley Match”



All better!



(confirmed gain & directionality with a pair of amateur radios)