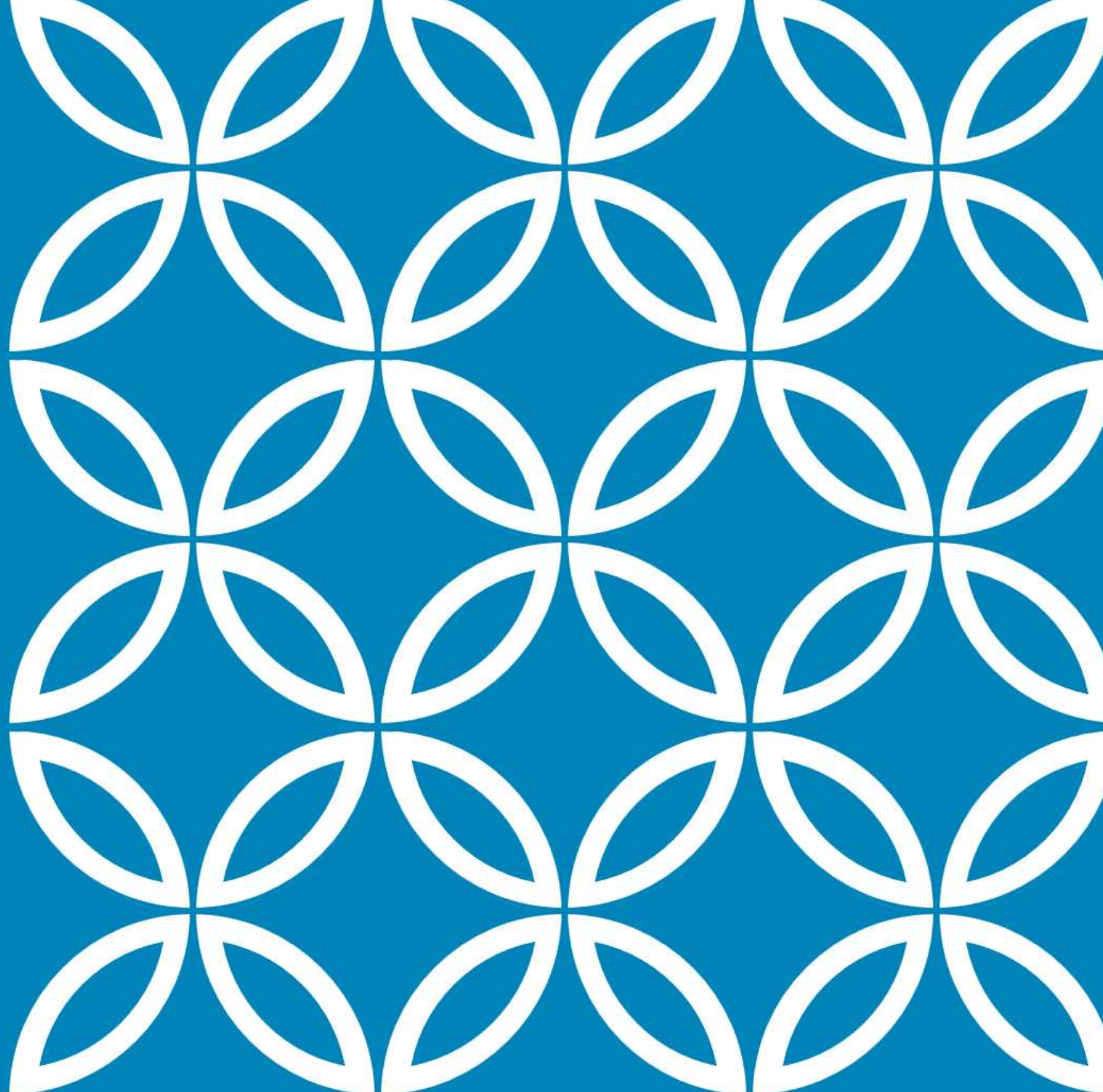
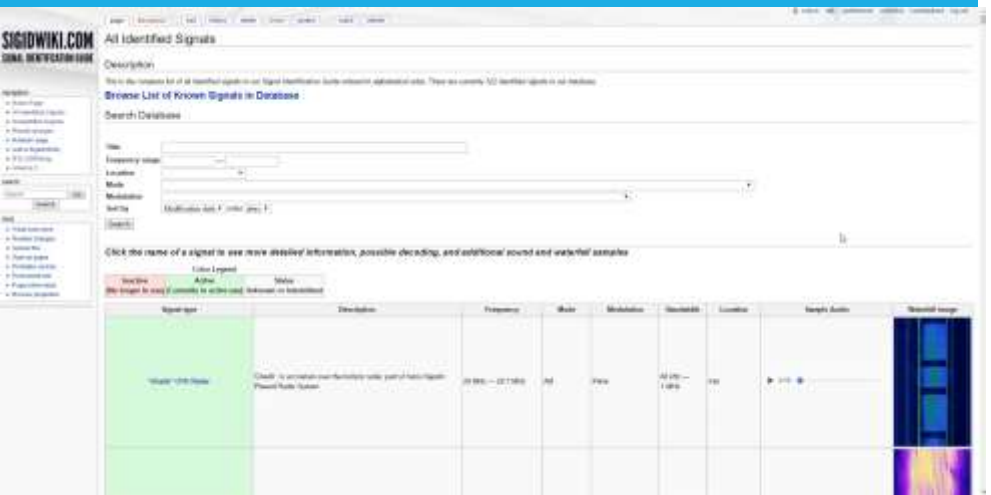
THE WORLD OF LOW COST SOFTWARE DEFINED RADIO

By Carl Laufer



WHO AM I



Running the RTL-SDR.com blog since 2013

Collecting stories relating to ultra cheap radio

Redesigned the RTL-SDR dongle for improved SDR performance

Started sigidwiki.com, a collection of signals

www.rtl-sdr.com

WHAT IS THE RTL-SDR?

A very cheap RX software defined radio based on the RTL2832U chipset.

- Software defined radio? Basically a tuner and ADC. All demod is done in software.

Originally (and still is) a DVB-T TV Tuner

- Highly mass produced in China – very cheap

Hardware hackers found the SDR feature

- Originally designed for FM radio reception

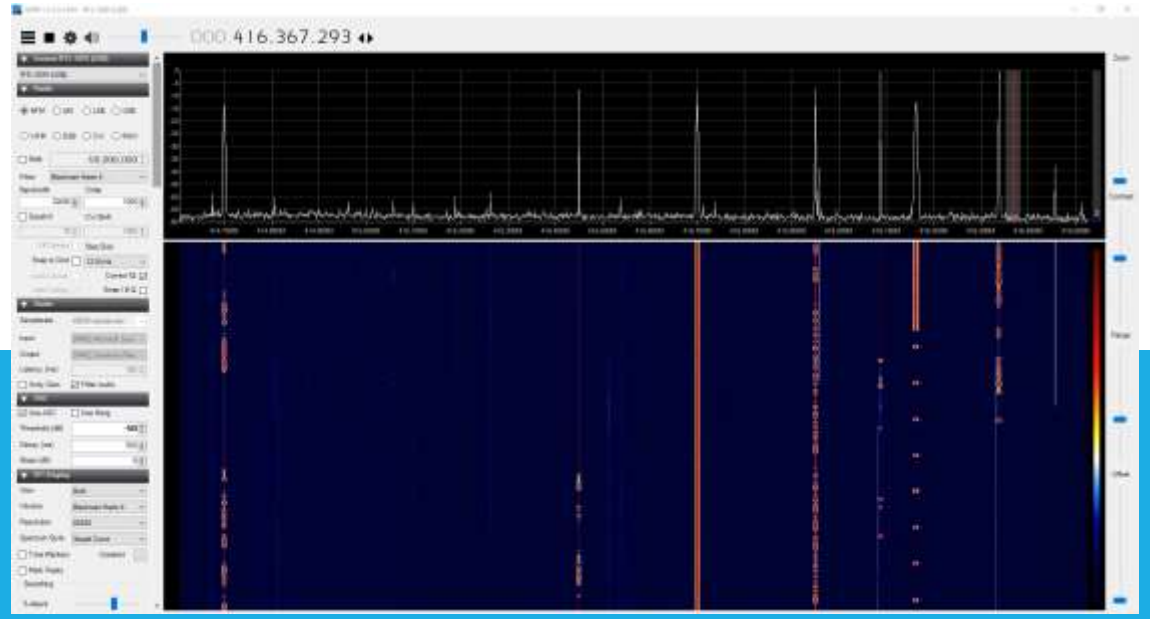
They wrote custom drivers to extend it's frequency range

Suddenly it's an extremely versatile receiver.

- Can receive/demod/decode almost anything from 24 – 1.8 GHz for $10 USD.

Opened up a whole new world of experimentation.

- New (and old) blood returning to the radio scene.



WHAT IS THIS TALK ABOUT?

An overview or “literature review” on interesting applications for the RTL-SDR

Avoiding the “common” scanner applications, will be talking about the weirder and niche stuff.

There are a lot of applications, let’s get started!

COMMON SCANNER APPLICATIONS FOR AN RTL-SDR

Amateur Radio

- HF, VHF, UHF, Digital, APRS, SSTV, Satellite

Analog EMS Communications

Digital EMS Communications

- P25, DMR, TETRA

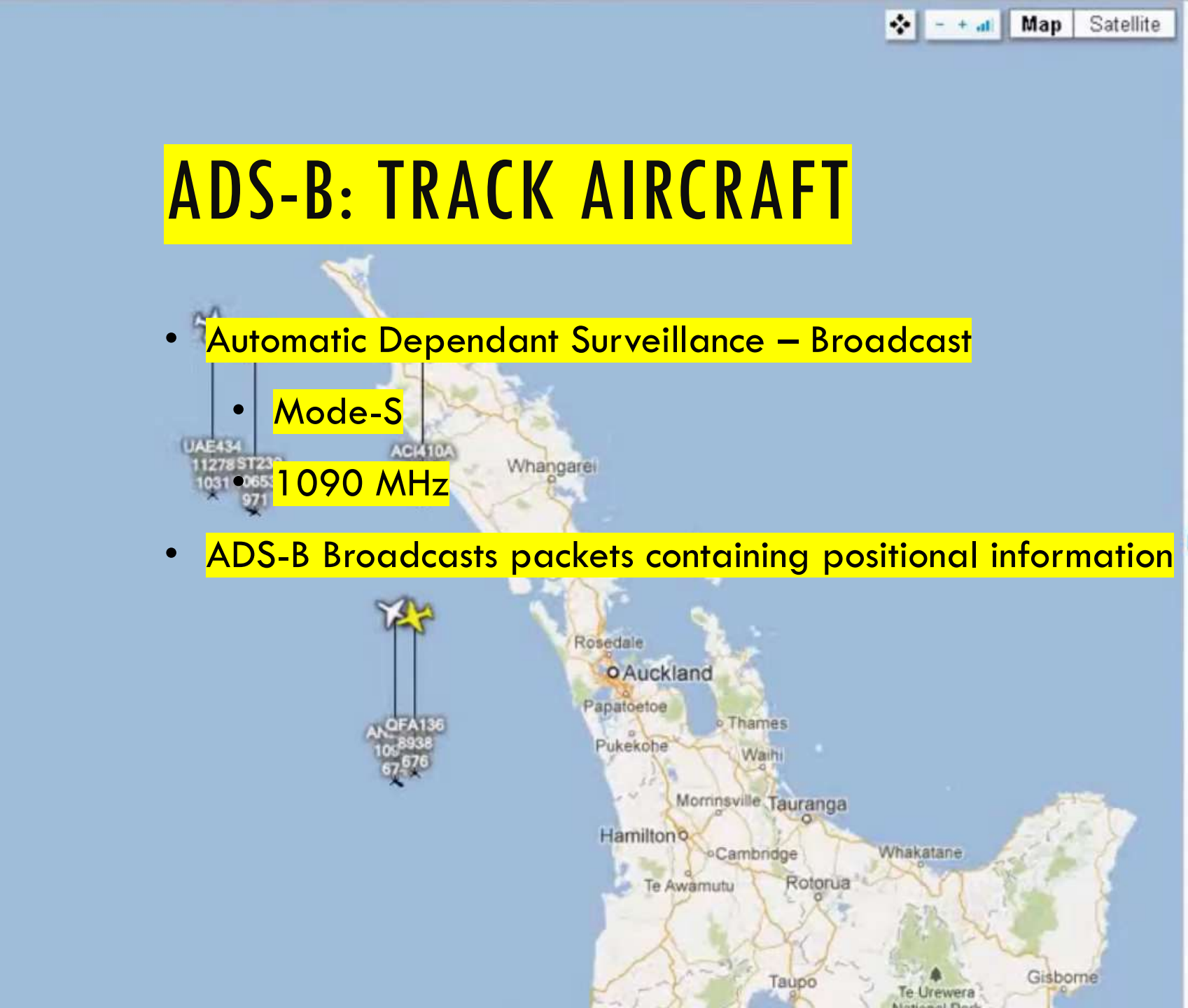
Trunked Radio

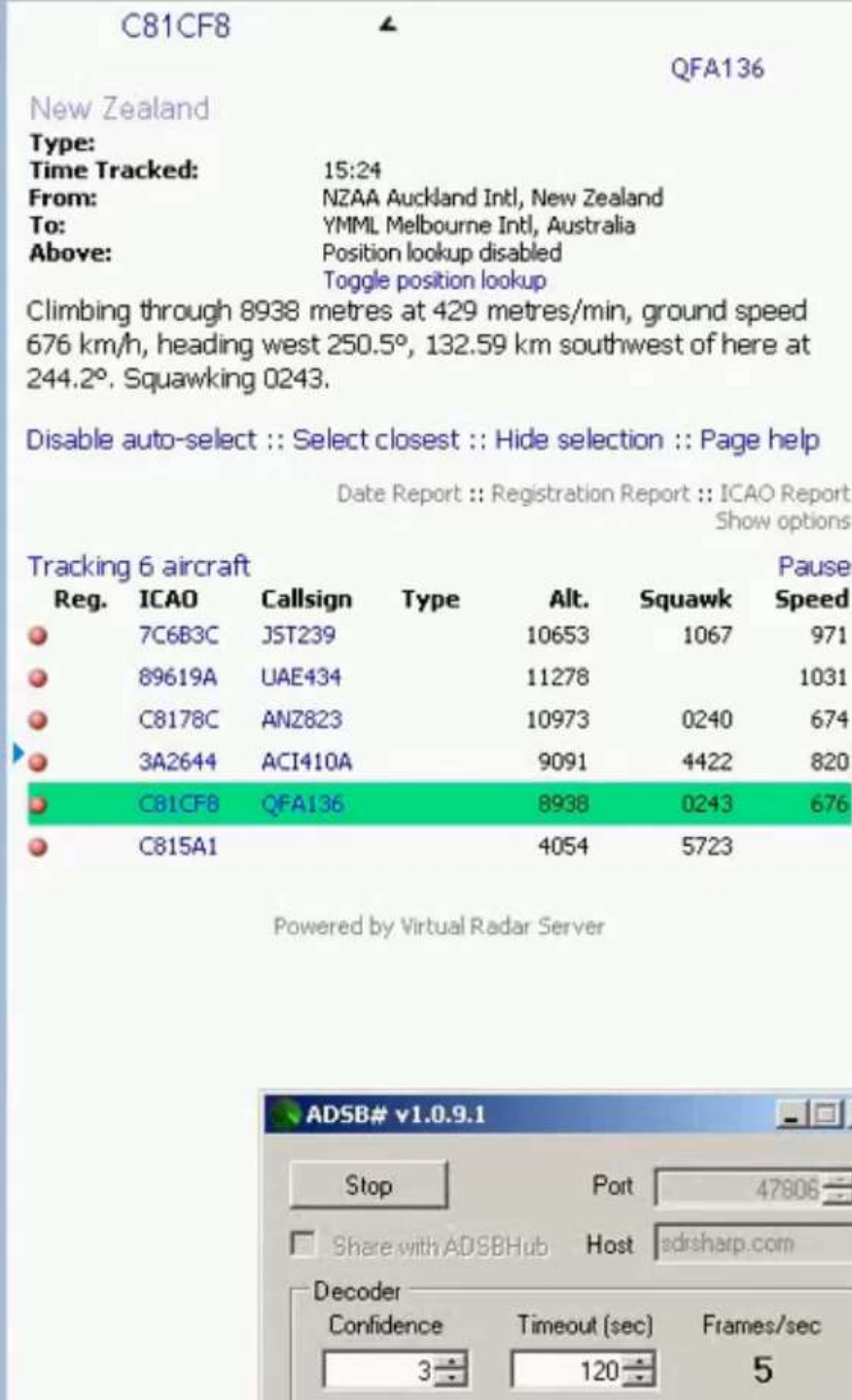
Air Traffic Control

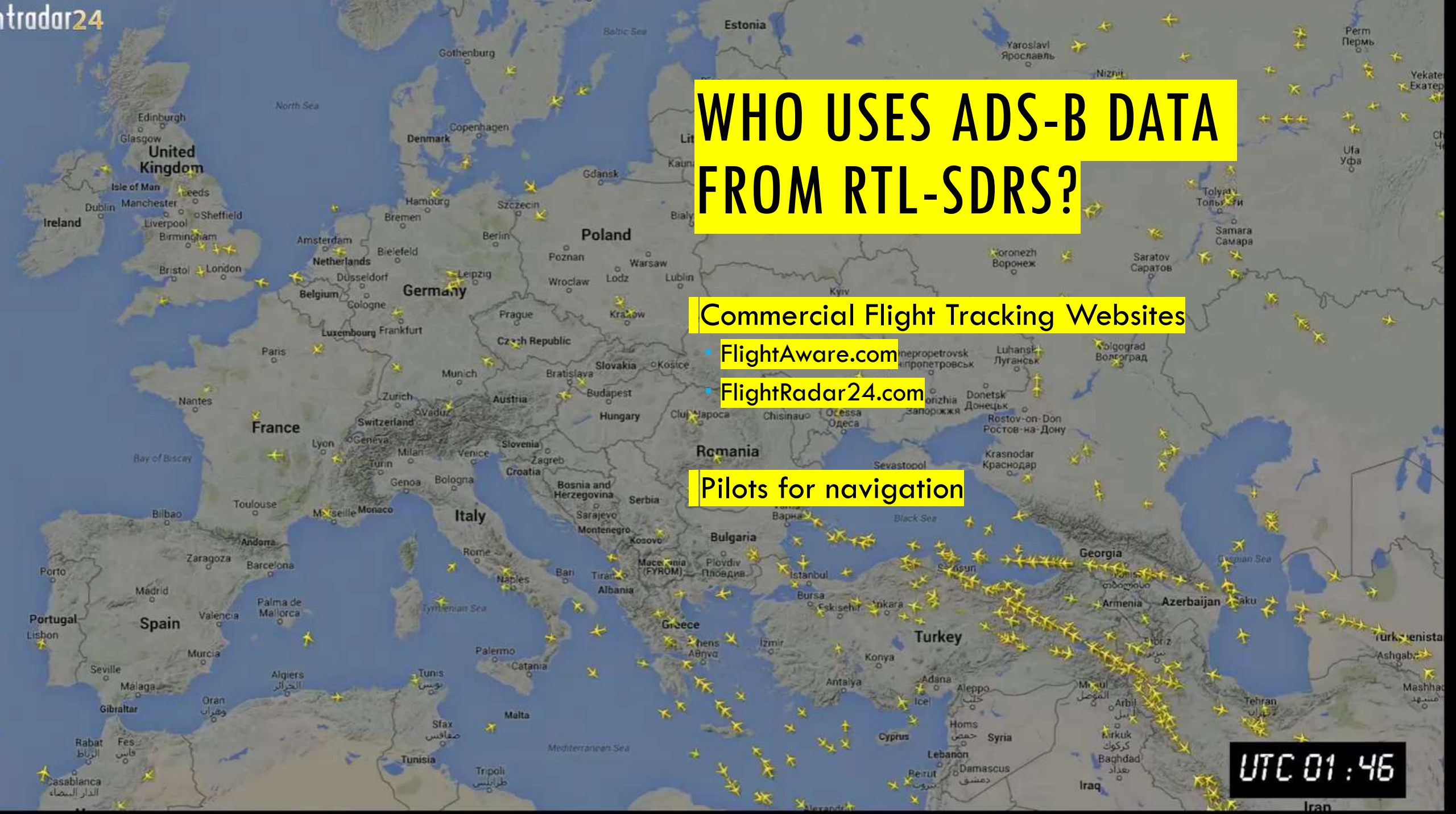

TRACKING AIRCRAFT AND BOATS
Hannover

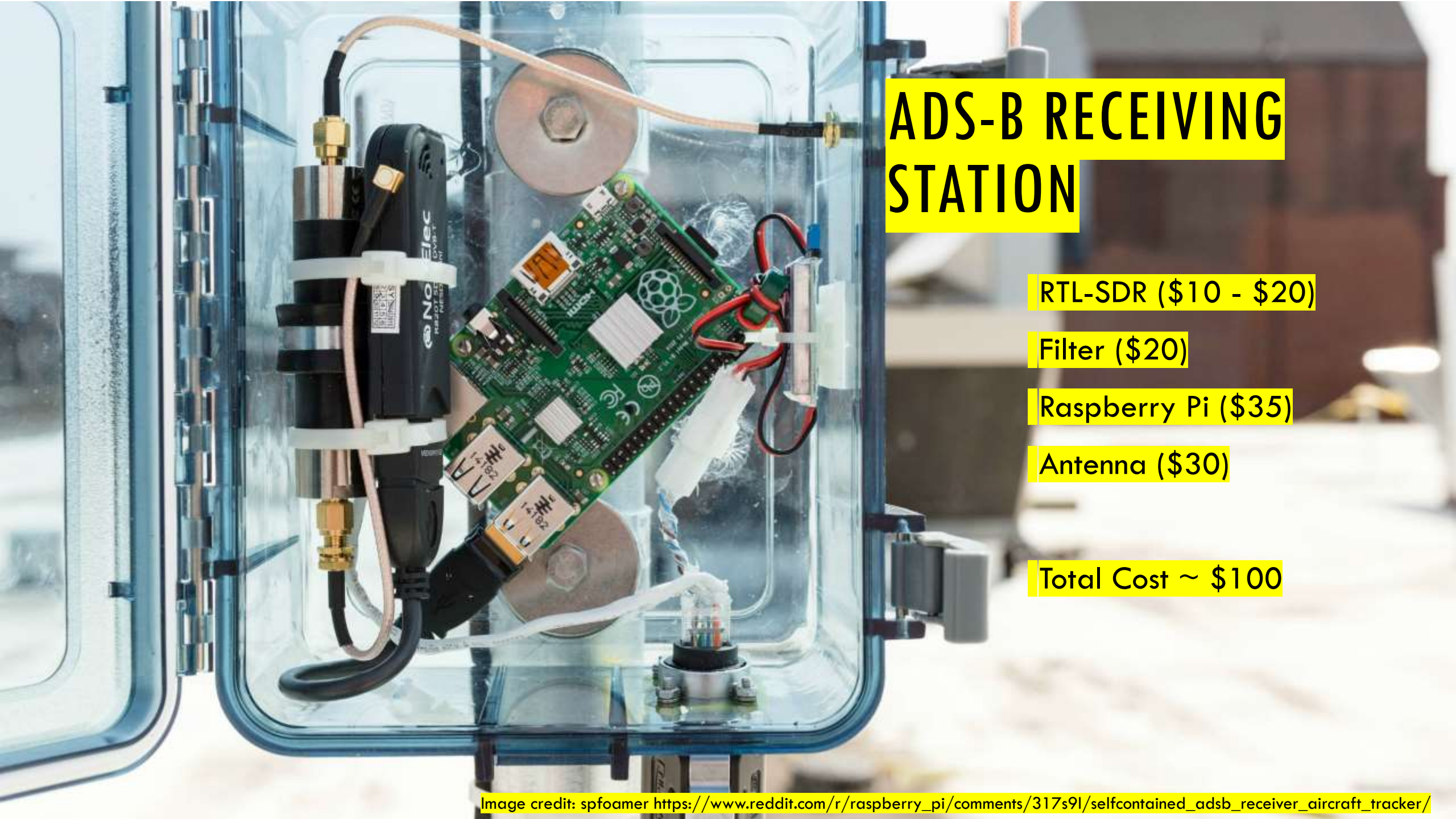
ADS-B: TRACK AIRCRAFT

- Automatic Dependant Surveillance – Broadcast
  - Mode-S
  - 1090 MHz
- ADS-B Broadcasts packets containing positional information






WHO USES ADS-B DATA FROM RTL-SDRS?
Commercial Flight Tracking Websites
FlightAware.com
FlightRadar24.com
Pilots for navigation
UTC 01:46



ADS-B RECEIVING STATION

- RTL-SDR ($10 - $20)
- Filter ($20)
- Raspberry Pi ($35)
- Antenna ($30)

Total Cost ~ $100

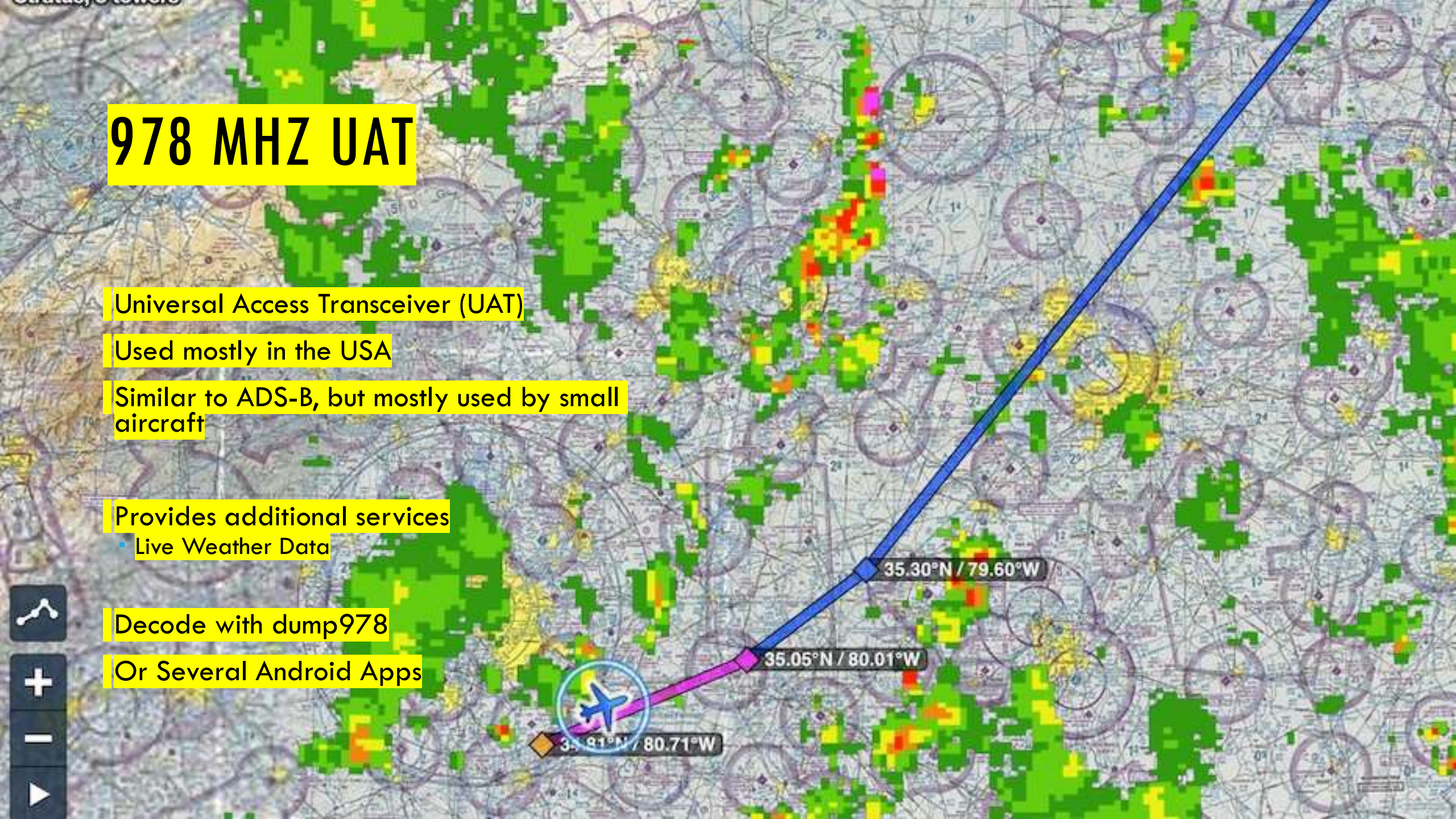
Image credit: spfoamer https://www.reddit.com/r/raspberry_pi/comments/317s9l/selfcontained_adsb_receiver_aircraft_tracker/

978 MHZ UAT

- Universal Access Transceiver (UAT)
- Used mostly in the USA
- Similar to ADS-B, but mostly used by small aircraft

- Provides additional services
  - Live Weather Data

- Decode with dump978
- Or Several Android Apps



STRATUX

- Small plane pilots are using RTL-SDRs in the cockpit
- Professional ADS-B/UAT equipment costs thousands of bucks
- Stratux costs a few hundred dollars only

- RTL-SDR runs on a Raspberry Pi. Raspberry Pi connects to a tablet which is running navigation software.

- stratux.me

AUTOMATIC IDENTIFICATION SYSTEM (AIS)

Similar to ADS-B but for Boats

Used in collision avoidance

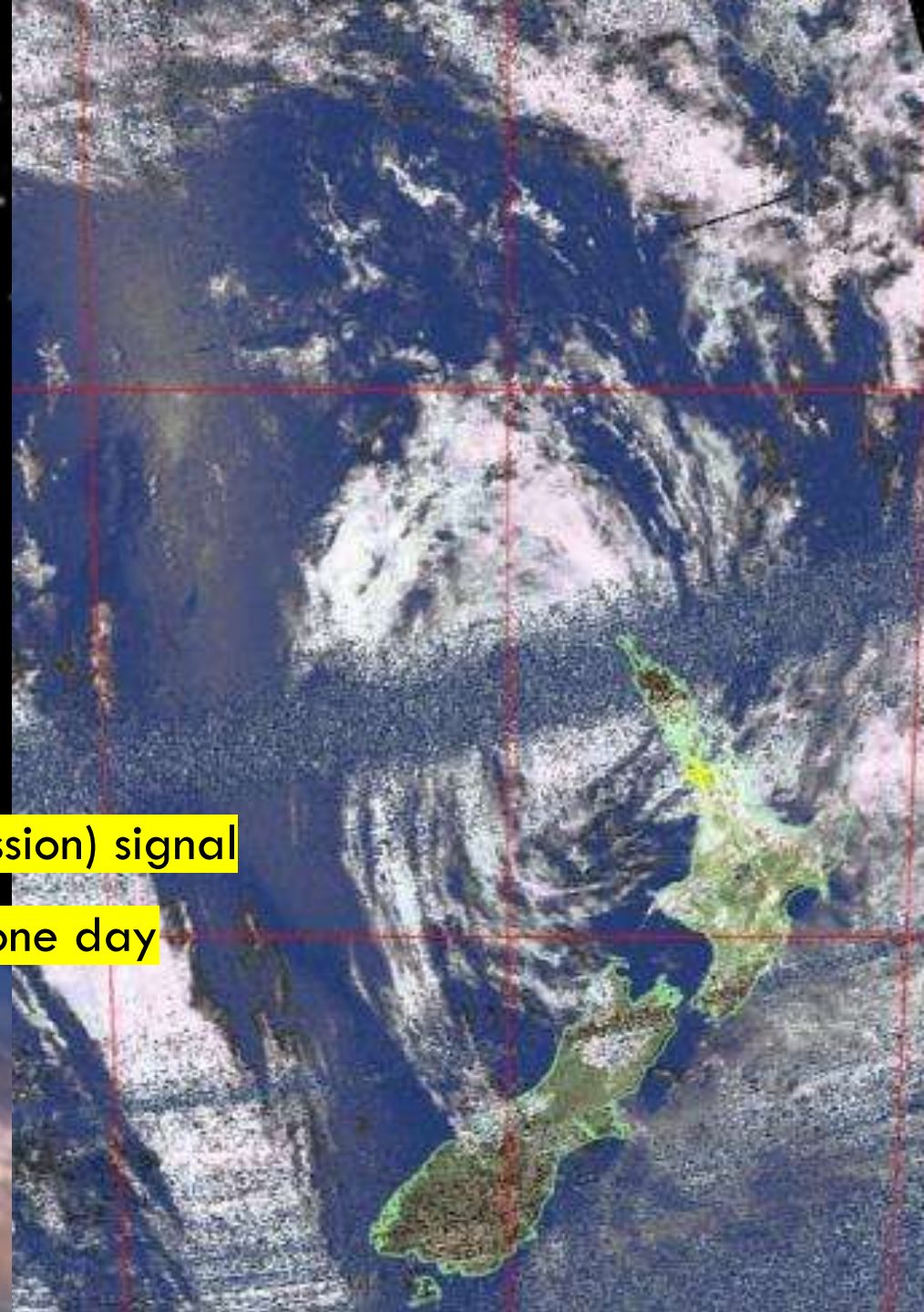
Receive and plot on a map just like ADS-B

Like Stratux, some small boat owners are using RTL-SDR + Raspberry Pi units onboard to get AIS data.

LEO SATELLITES

NOAA WEATHER SATELLITES

- Receive live weather images
- Three active satellites
  - NOAA 15 – 137.6200 MHz
  - NOAA 18 – 137.9125 MHz
  - NOAA 19 – 137.1000 MHz
- Transmits an analogue “APT” (Automatic Picture Transmission) signal
- Will pass over every location on earth several times in one day



METEOR M-N2 WEATHER SATELLITE

- Russian weather satellite
  - Launched on July 8, 2014
- Broadcasts at 137.925 MHz
- Significantly higher resolution images that NOAA satellites
  - Uses digital signals
  - LRPT “Low Rate Picture Transmission”

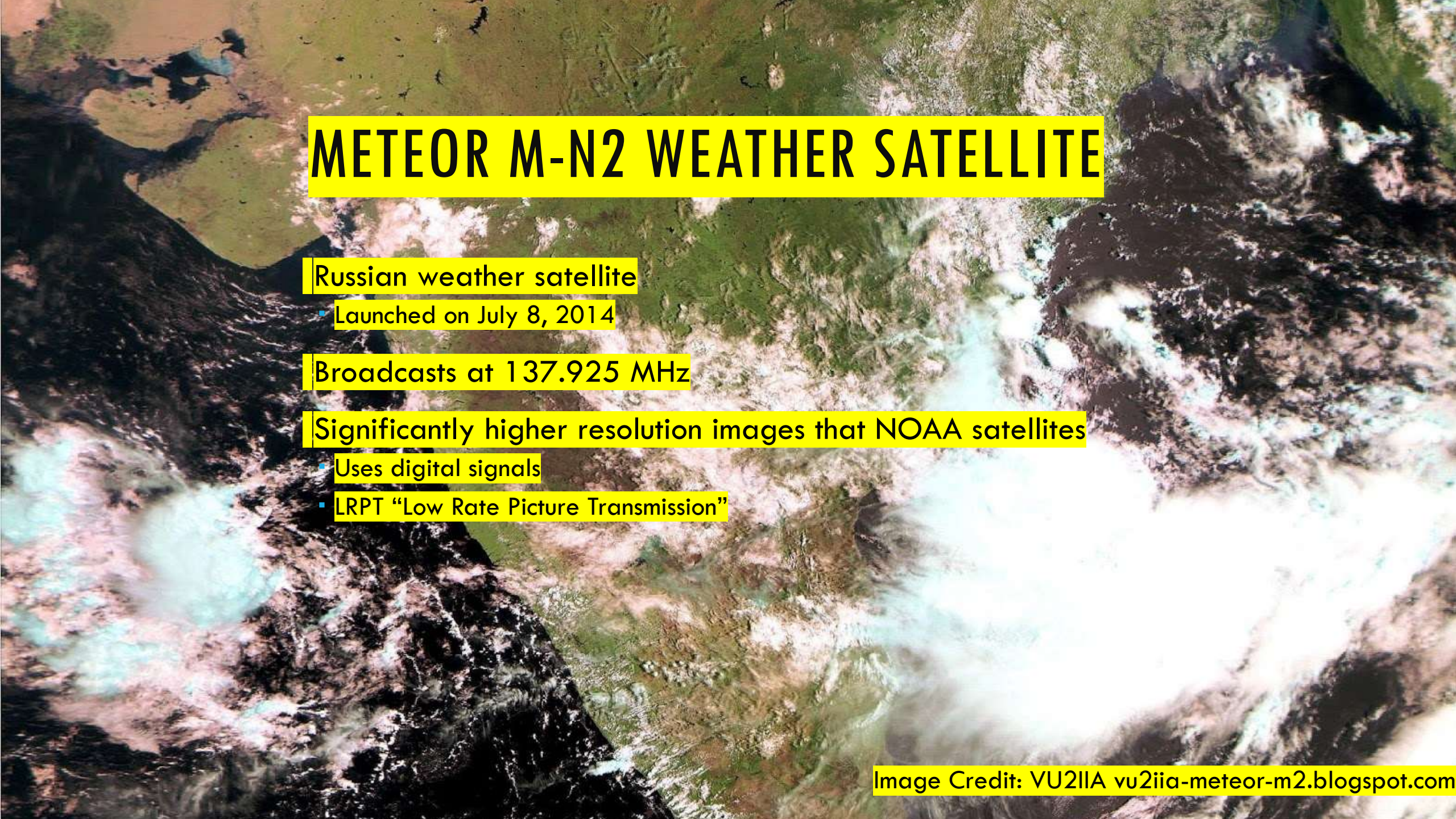
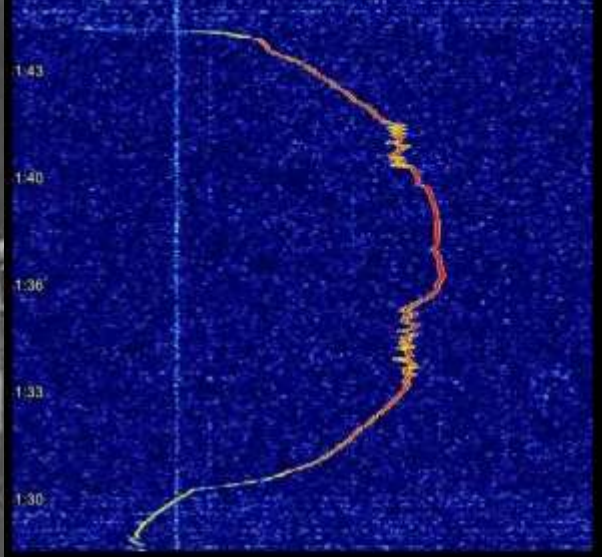


Image Credit: VU2IIA vu2iia-meteor-m2.blogspot.com

Receiving Dead Satellites

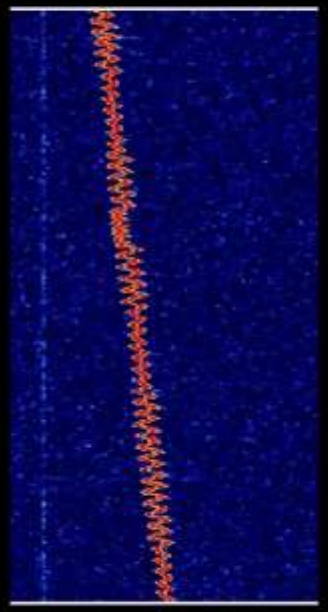
- Some very old decommissioned satellites can resurrect themselves
- Chemical reaction in the batteries
  - Degradation due to thousands of sun cycles
- After the reaction the batteries short
  - Power can pass through while the satellite is in sunlight



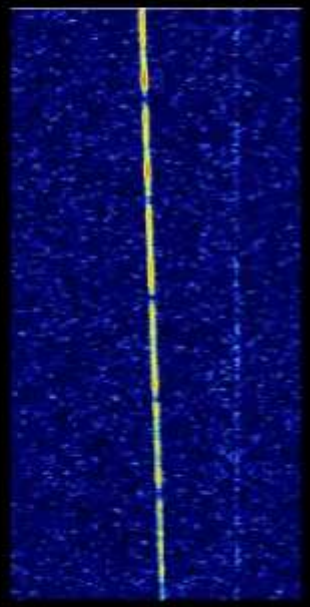
NOAA 19

Image credit: happysat

Transit 5B

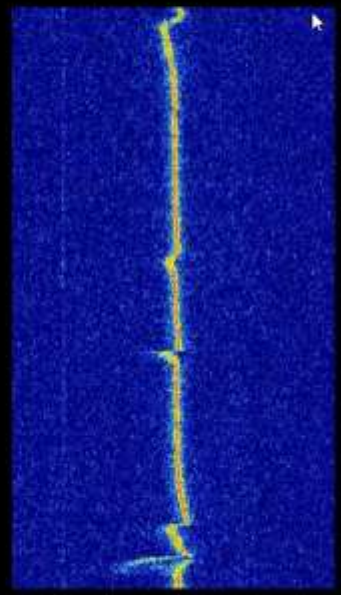


Transit 5B



LES-1

Tiros-1



Aloutte

SATNOGS

Vast increase in amateur radio satellites and cubesats launching

Not enough ground stations to collect data

SatNOGS solution: 3D printed antenna rotator system

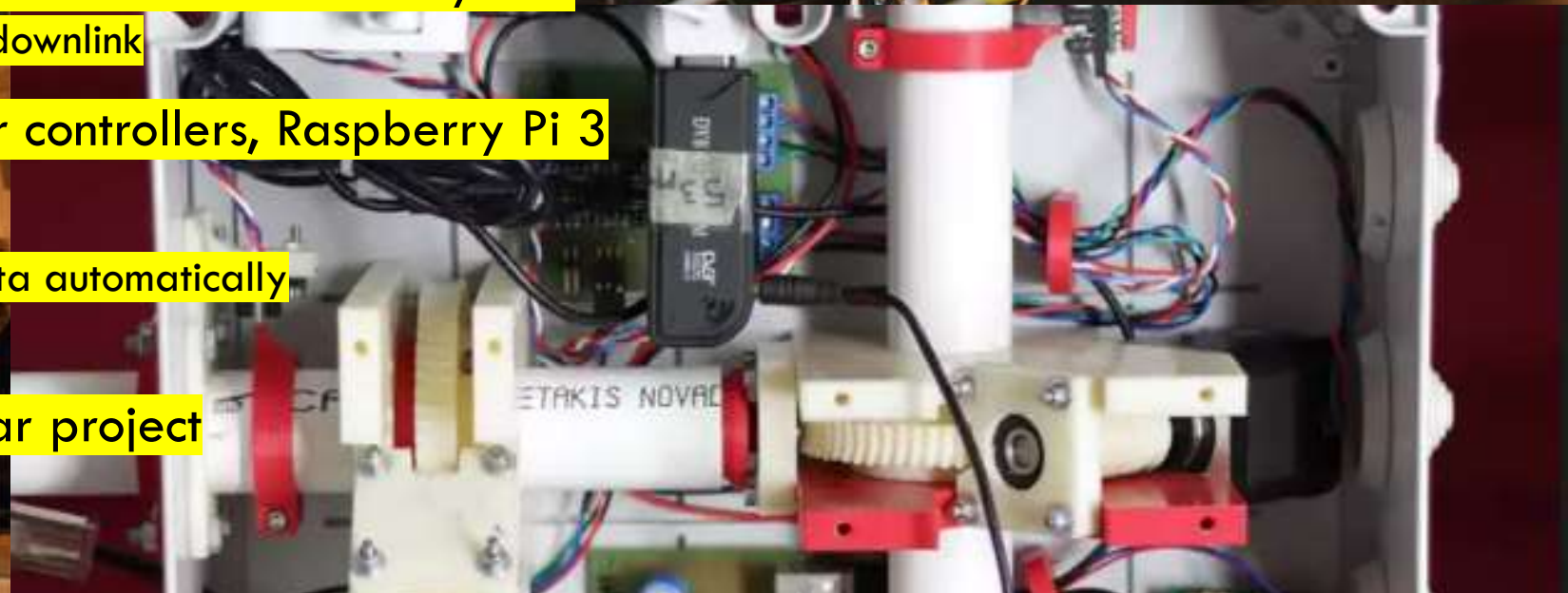
- Automatic satellite tracking and downlink

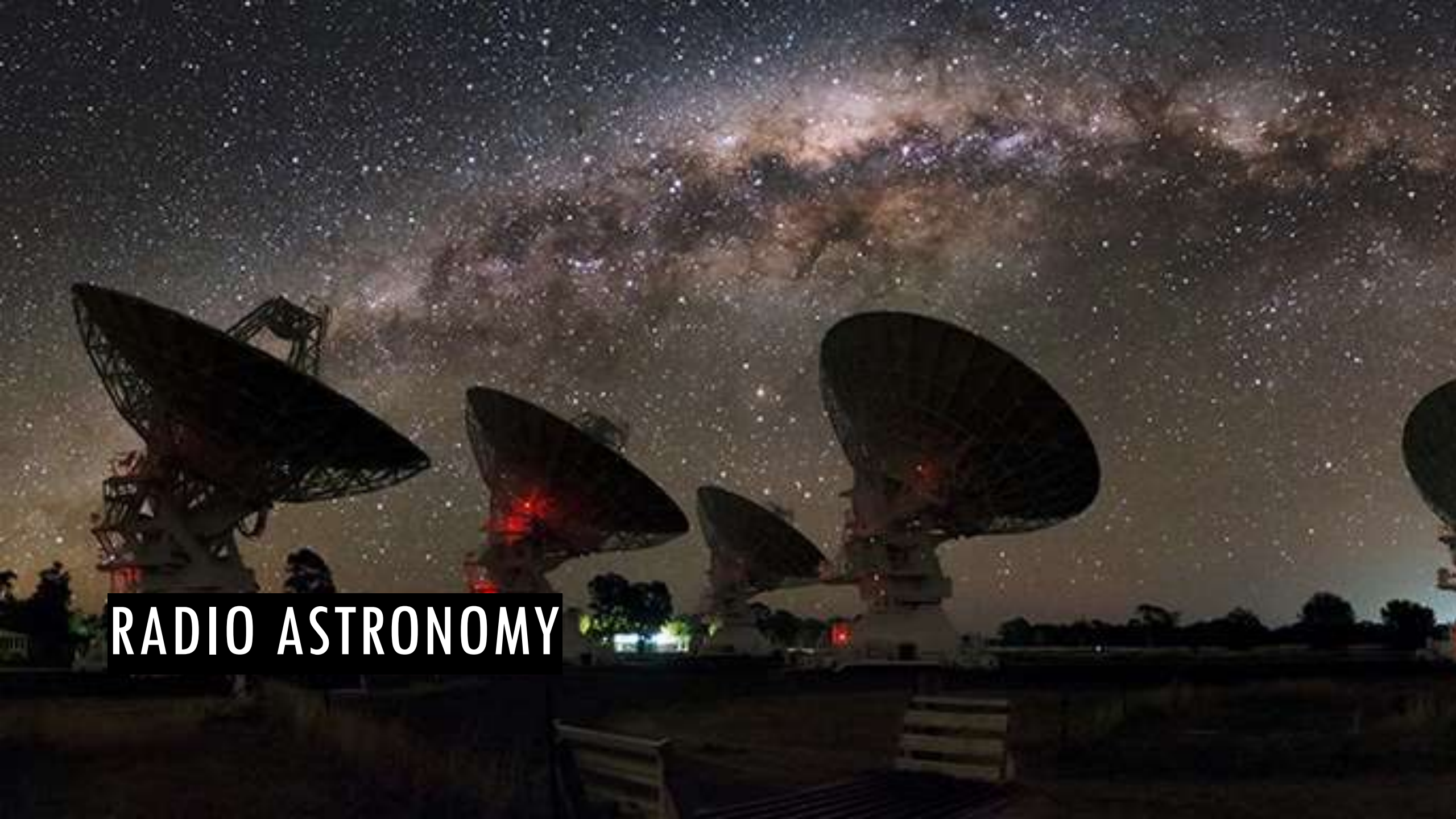
Inside: RTL-SDR, gears, motor controllers, Raspberry Pi 3

Connected to internet

- Collects and uploads satellite data automatically

ThumbNet/ThumbSat a similar project




RADIO ASTRONOMY

FORWARD METEOR SCATTER DETECTION

Use the RTL-SDR as a meteor detector/counter

- Meteors leave behind trails of ionized air which is RF reflective

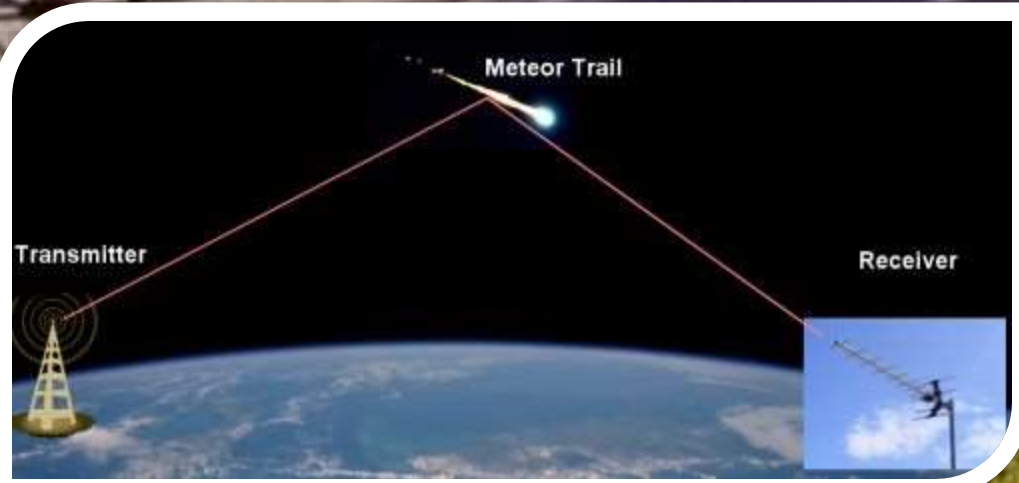
Point a directional antenna at the sky

- Listen for reflections from powerful transmitters hundreds of kilometres away

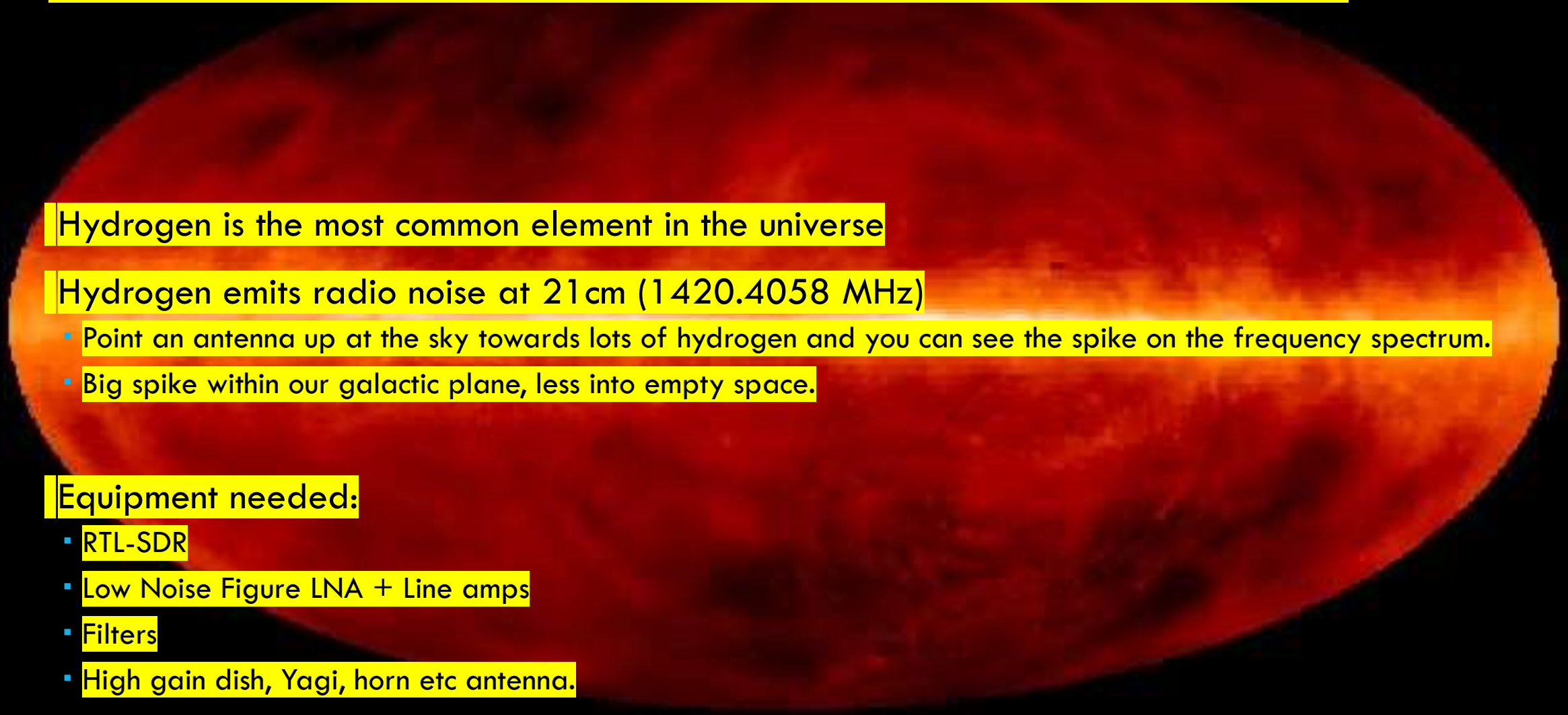
Transmitters you can use include

- Graves Radar (Europe) or other radar
- TV towers

livemeteors.com



HYDROGEN LINE & GALACTIC PLANE DETECTION



Hydrogen is the most common element in the universe

Hydrogen emits radio noise at 21cm (1420.4058 MHz)

- Point an antenna up at the sky towards lots of hydrogen and you can see the spike on the frequency spectrum.
- Big spike within our galactic plane, less into empty space.

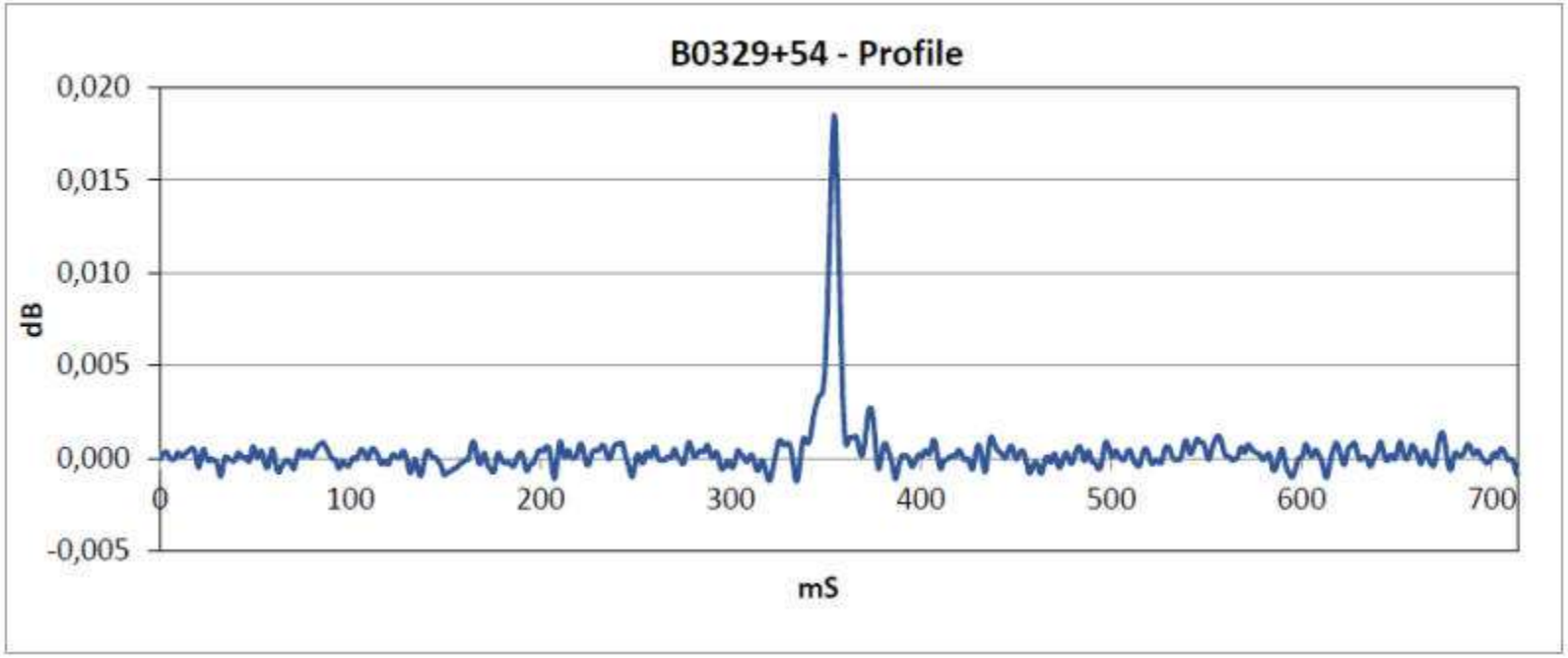
Equipment needed:

- RTL-SDR
- Low Noise Figure LNA + Line amps
- Filters
- High gain dish, Yagi, horn etc antenna.

DETECTING PULSARS

Peter East and Guillermo Gancio (30M dish at the Argentine Institute for Radio Astronomy)

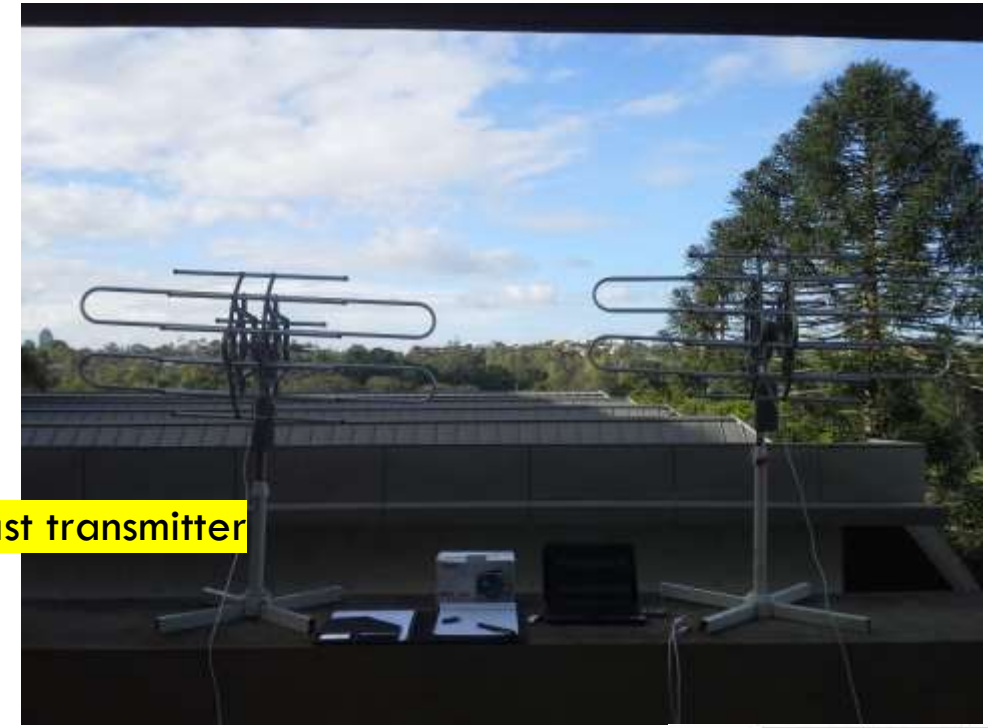
- Rotating Neutron Star
- Wideband noise bursts over a wide frequency range
- RTL-SDR Receiver records raw IQ data
- Mathematical algorithms required to detect the pulsar
- neutronstar.joataman.net



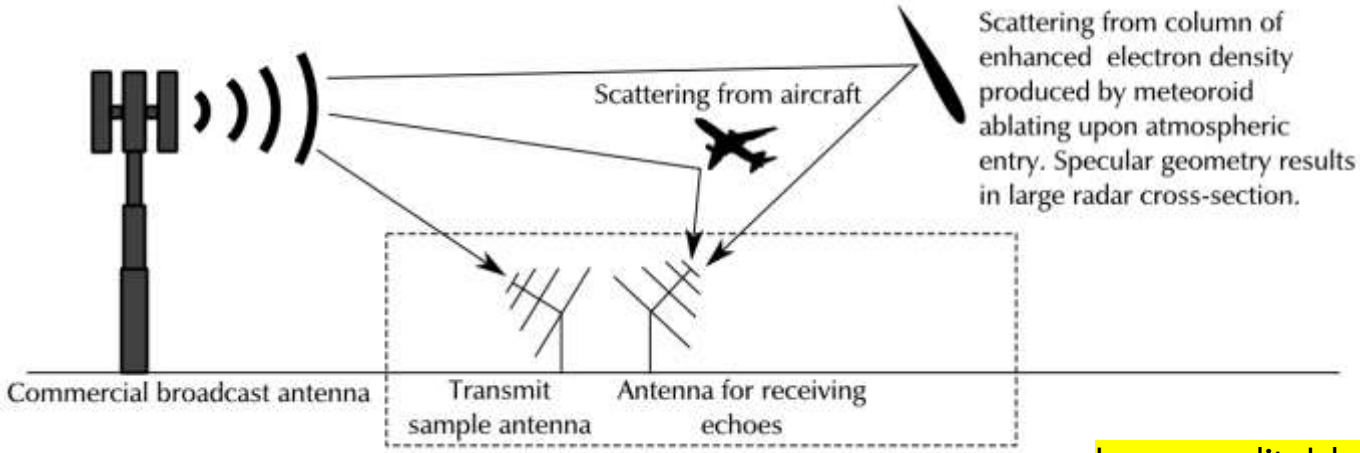
Andrea Dell'Immagine (IW5BHY)


QRM DETECTING, DIRECTION FINDING, RADAR

PASSIVE RADAR



- Similar to meteor detection
  - Uses reflections from a powerful broadcast transmitter
- But if you use two antennas
  - You can get a 2D Radar view



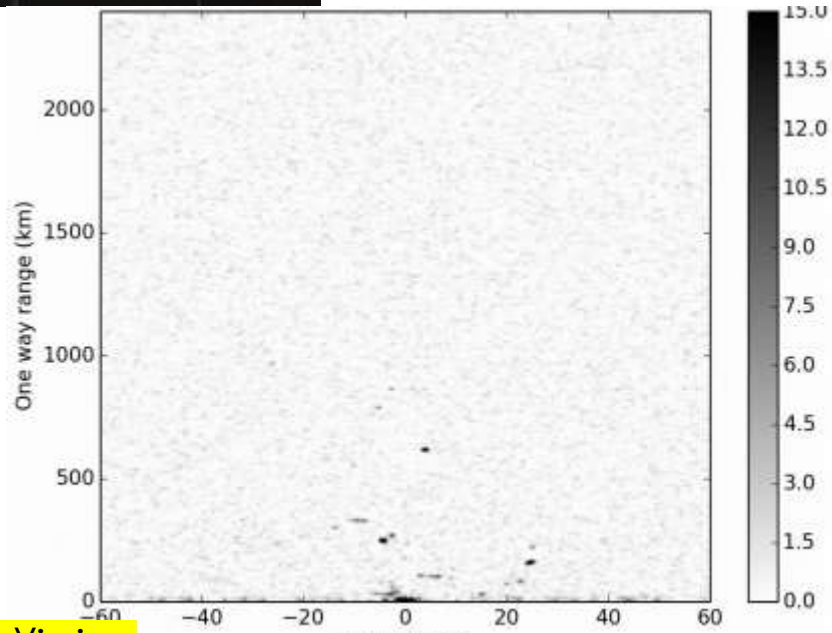
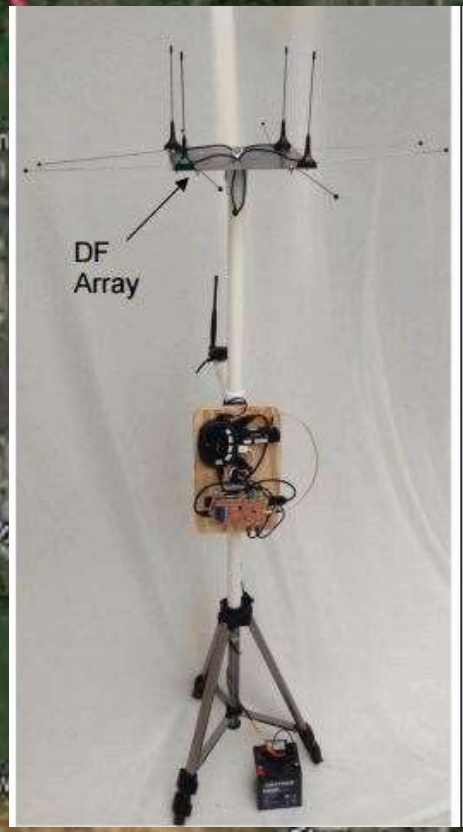
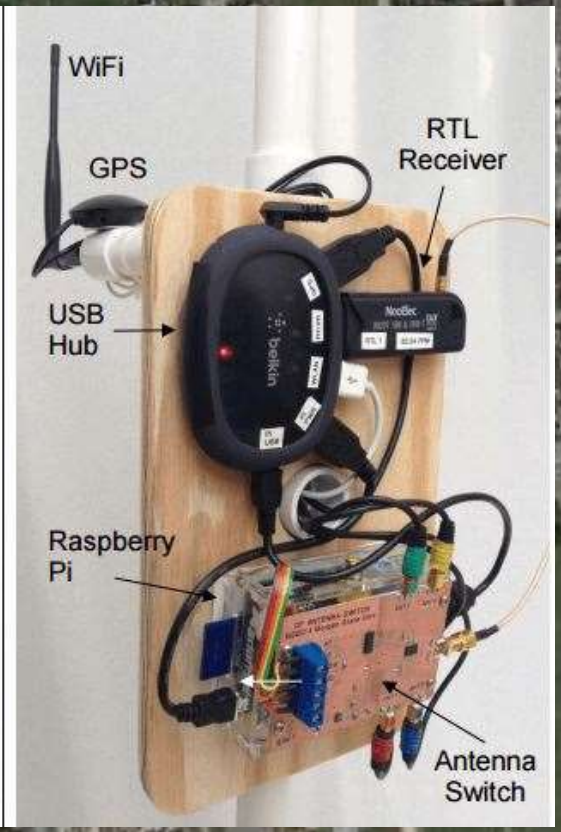


Image credit: Juha Vierinen

SIGNAL DIRECTION FINDING

- RasHAWK System
- Based on Raspberry Pi's and REDHAWK DSP
- Uses antenna switching
- Determines the signal bearing
- Combine several units to pinpoint the transmitter





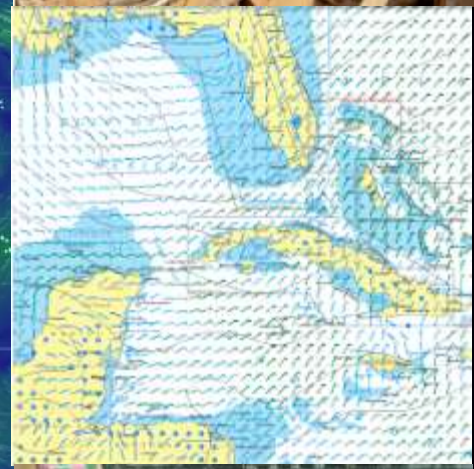
QRM/NOISE DETECTION AND LOCATING

- Tim Havens “Driveby” System: QRM Detector
- Uses multiple RTL-SDR dongles running on an Odroid XU3
  - Scans multiple bands
- Log QRM levels together with GPS data
  - Find the hotspots on a heatmap
- Source found: Power pole with broken ground connection


L-BAND SATELLITES

OUTERNET Search in folders: Weather

RECEIVING THE OUTERNET



One way (download only) satellite filecasting service

- Uses Inmarsat/Alphasat satellites on L-band

What data can you receive?

- Latest News
- Weather Updates
- Amateur Radio repeater repeats (ISS APRS, AMSAT etc)
- Wikipedia Articles
- Grib files (for mariners at sea)
- Free books

Good for disaster preppers, sailors, remote areas, countries with censored internet, third world countries.

Outernet use RTL-SDR based receivers

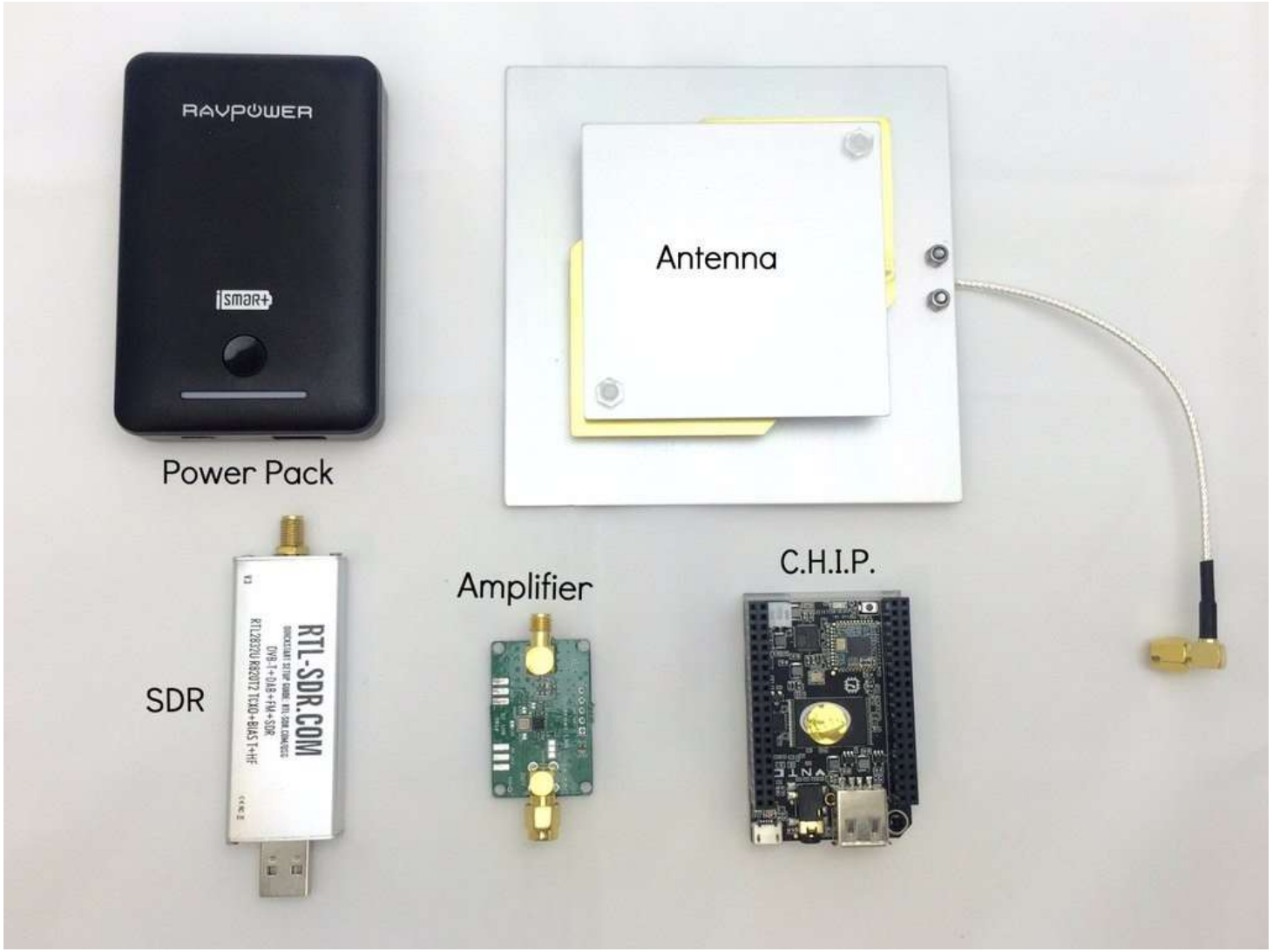
earth

WHAT DO YOU NEED TO RECEIVE OUTERNET

- RTL-SDR v3 or E4000 dongle (with bias tee)
- An LNA (with filter)
- L-band 1.5 GHz satellite antenna (such as a patch or dish)
- C.H.I.P Computer

- Outernet are working on a fully integrated solution

www.outernet.is



L-BAND SATELLITES: INMARSAT SAFETYNET

Inmarsat STD-C “SafetyNET” safety message broadcast

Mainly weather, search and rescue, incident reports, submarine cable deployments, military exercises and pirate warnings for mariners.

- 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.
- DUTY ENGINEER ONBOARD AN UNDERWAY PRODUCT TANKER DISCOVERED THREE ROBBERS IN THE ENGINE ROOM NEAR THE INCINERATOR SPACE. THE ROBBERS RAN TO THEIR BOAT. A SEARCH WAS CARRIED OUT. NO ROBBERS FOUND ON BOARD AND NOTHING REPORTED STOLEN.

Software

- www.inmarsatdecoder.com
- Tekamanoid http://www.tekmanoid.com/egc.shtml

L-BAND SATELLITES: IRIDIUM

Iridium is a global satellite service with over 72 satellites

- Provides services such as global pagers, satellite phones, fleet tracking and management, and various services for emergency, aircraft, maritime and covert military as well.

Security researchers Stefan “Sec” Zehl and Schneider have decoded Iridium

- Can receive calls and pager messages
- In their talk they demonstrate intercepting a call from the 310th airlift squadran C-37 military aircraft.
- Easy, but not too easy to listen in on.

L-BAND SATELLITES: EXAMPLE OF WHAT STEFAN AND SCHNEIDER RECEIVED

"heli on route. Also what batteries do you require? Joe, get on tacsat to me asap, your grid is wrong, should be 40 xxxx 89681 21960. You are going 8km the wrong way. …our arcs are not on the target. Grid I have of you is xxxx 4882 and enemy location xxxx 4804. J2 indicates Op compromise. Extract immediately. Act via HF."

"call socrates for information updates we have a quality target. After Germany, call socrates on blue comm and get ready to work. there is a red scorpion on sail. You need to call xxxx or xxxx. we this it is best if you call from xxxx or xxxx. Tell the bartender they need to talk to us before they can make the payment. in any case you must pass germany to do it listen to White, open long man! report before or at Venezuela"


RF SECURITY

GATHERING ENTROPY VIA ATMOSPHERIC NOISE

A computer cannot generate true random numbers

- Only pseudo-random

True randomness can be obtained from mouse and keyboard movements

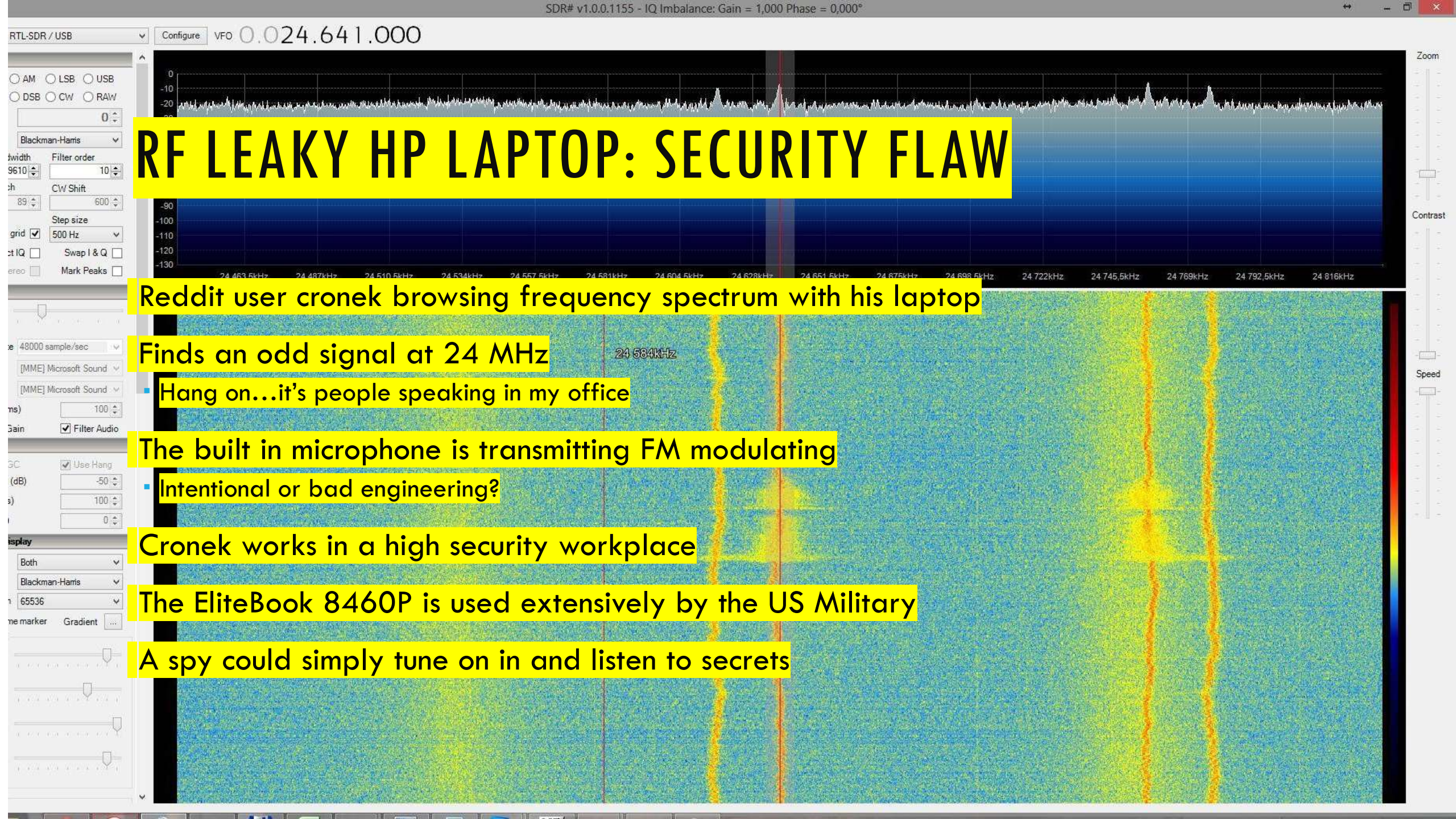
- But what about embedded computers (e.g. routers, IoT devices) with no inputs?

True randomness is needed for cryptography and securing systems.

- If the keys are not truly random, they can be guessed/calculated.

An RTL-SDR program called rtl_entropy can be used to gather true random numbers

- Gather from atmospheric noise (static). Galactic radiation, lightning.


SDR# v1.0.0.1155 - IQ Imbalance: Gain = 1,000 Phase = 0,000°
RTL-SDR / USB
Configure
VFO 0.024.641.000
AM LSB USB
DSB CW RAW
Blackman-Harris
Filter order
CW Shift
Step size
500 Hz
Swap I & Q
Mark Peaks
48000 sample/sec
[MME] Microsoft Sound
[MME] Microsoft Sound
Filter Audio
Use Hang
Both
Blackman-Harris
65536
Gradient
Zoom
Contrast
Speed
24 584kHz
RF LEAKY HP LAPTOP: SECURITY FLAW
Reddit user cronek browsing frequency spectrum with his laptop
Finds an odd signal at 24 MHz
Hang on…it's people speaking in my office
The built in microphone is transmitting FM modulating
Intentional or bad engineering?
Cronek works in a high security workplace
The EliteBook 8460P is used extensively by the US Military
A spy could simply tune on in and listen to secrets

GSM ANALYSIS AND DECODING

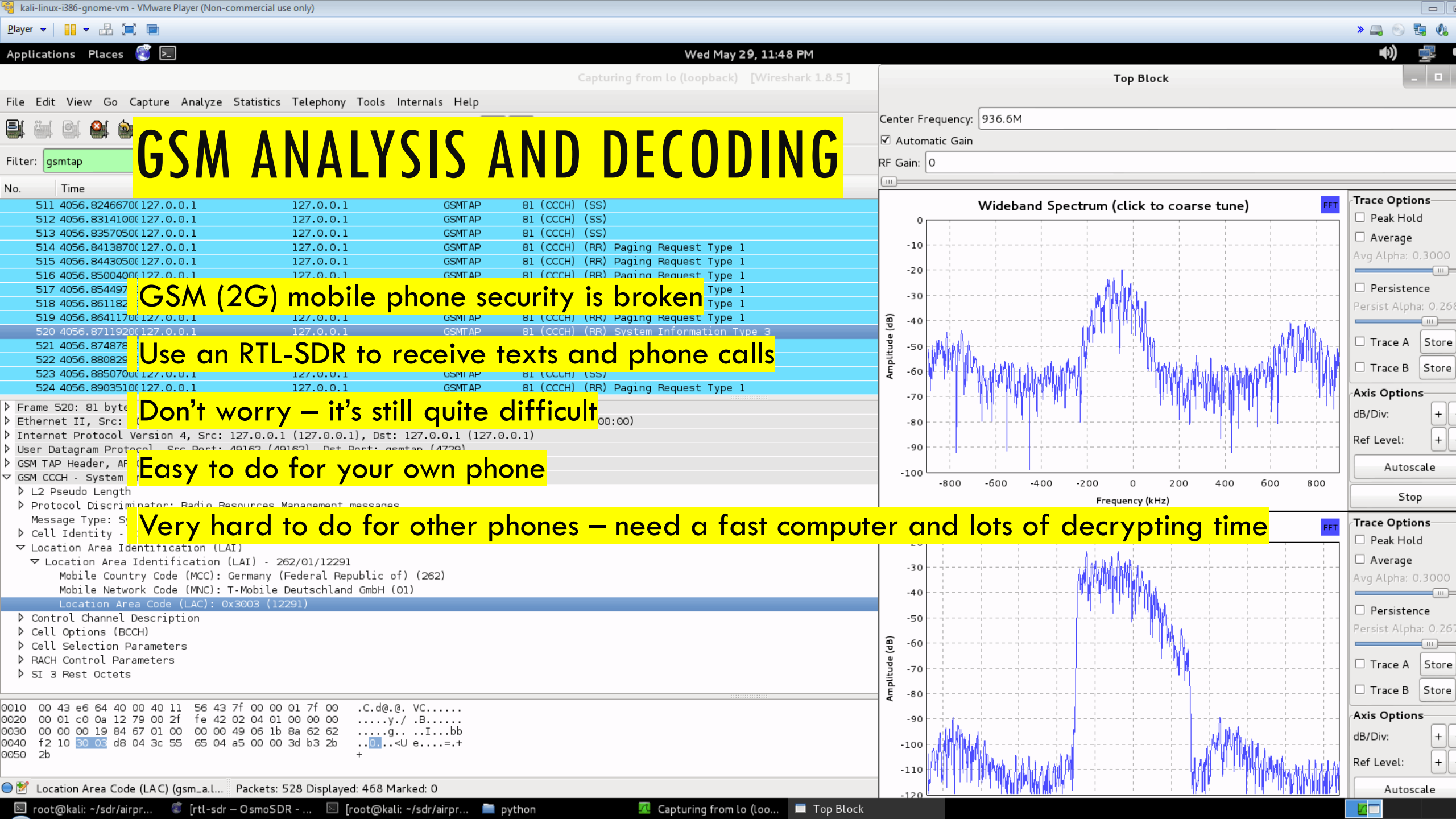
GSM (2G) mobile phone security is broken

Use an RTL-SDR to receive texts and phone calls

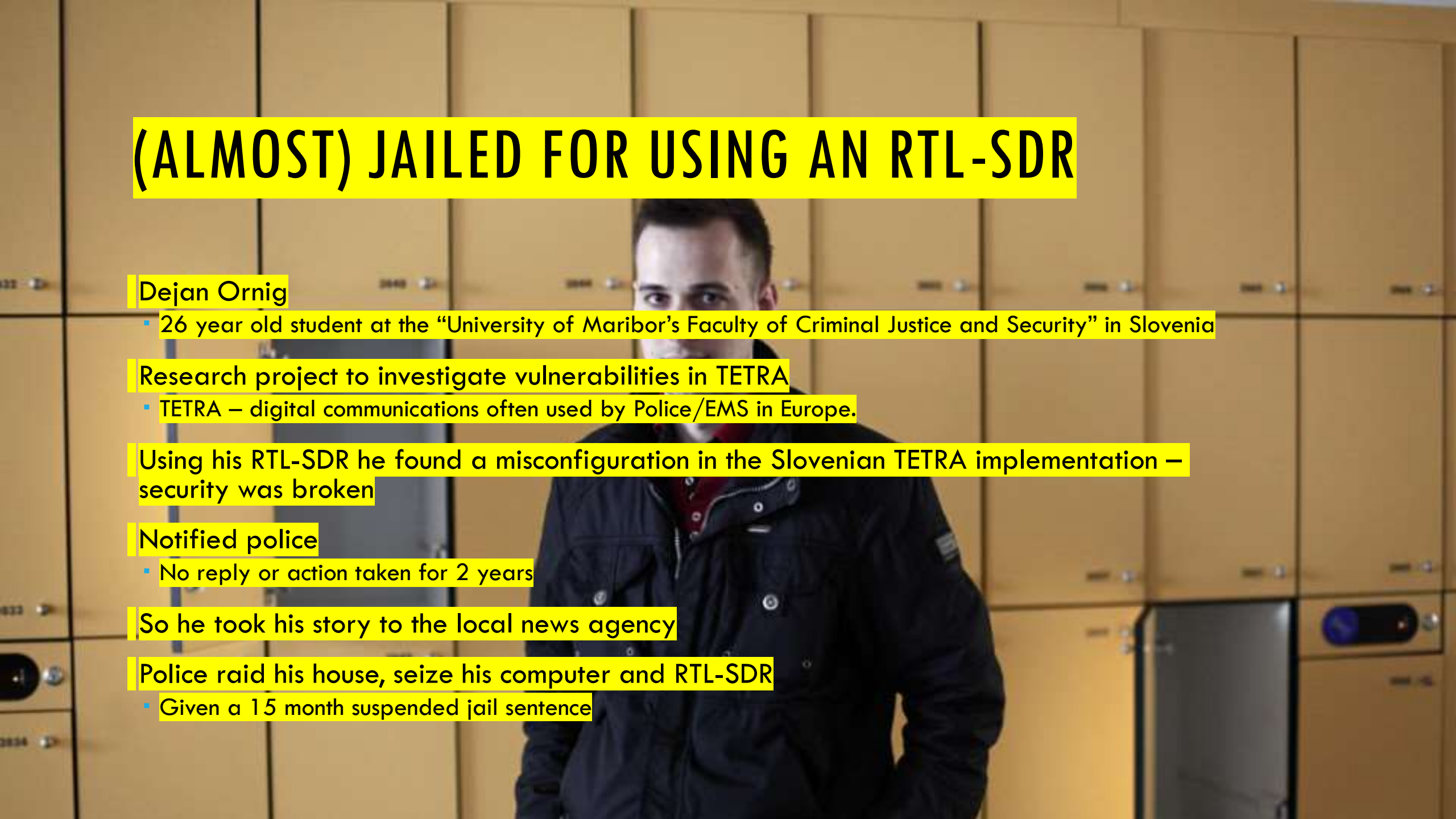
Don't worry – it's still quite difficult

Easy to do for your own phone

Very hard to do for other phones – need a fast computer and lots of decrypting time



(ALMOST) JAILED FOR USING AN RTL-SDR



Dejan Ornig

- 26 year old student at the “University of Maribor’s Faculty of Criminal Justice and Security” in Slovenia

Research project to investigate vulnerabilities in TETRA

- TETRA – digital communications often used by Police/EMS in Europe.

Using his RTL-SDR he found a misconfiguration in the Slovenian TETRA implementation – security was broken

Notified police

- No reply or action taken for 2 years

So he took his story to the local news agency

Police raid his house, seize his computer and RTL-SDR

- Given a 15 month suspended jail sentence

REVERSE ENGINEERING WIRELESS PRODUCTS

- Doorbells
- Temperature and weather sensors
- RC cars
- Ceiling fan
- Dog shock collars
- Wirelessly controlled AC power outlets
- Wireless door locks
- Home automation sensors and alarms
- IoT devices
- Portable traffic lights
- Public traffic displays
- Car doors
- Garage doors
- Implanted heart defibrillator

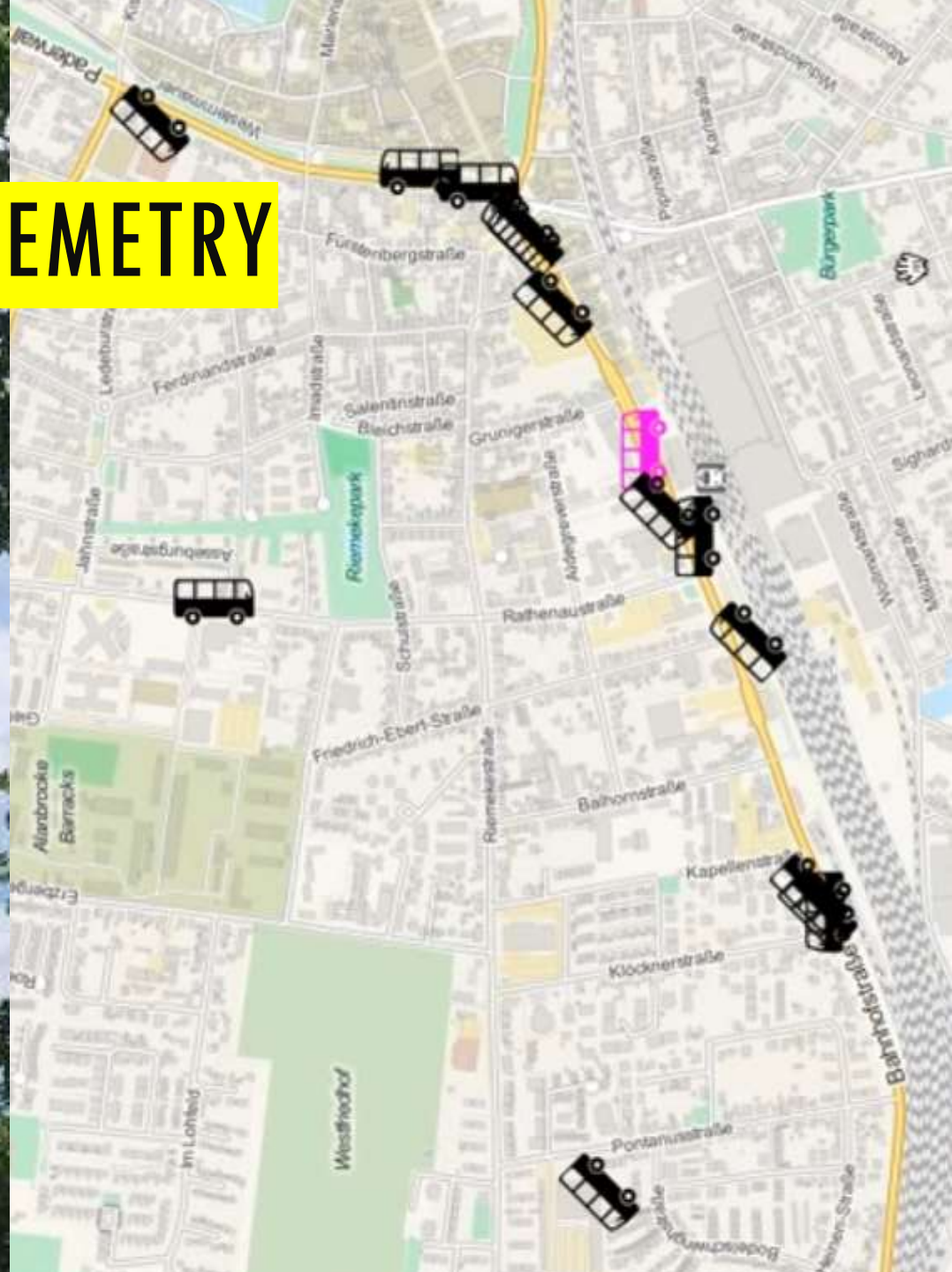
Image credit: Bastian Bloessl

REVERSE ENGINEERING BUS TELEMETRY

- Bus telemetry used in modern cities for signs at bus stops
  - Data transmitted wirelessly and is live

- Bastian Bloessl – Paderborn, Germany
  - Found a telemetry signal at 150 MHz

- Other telemetry broadcast methods like usiung subcarriers in broadcast FM are used in other countries.
  - See work by Oona Raissan in Helsinki, Finland.



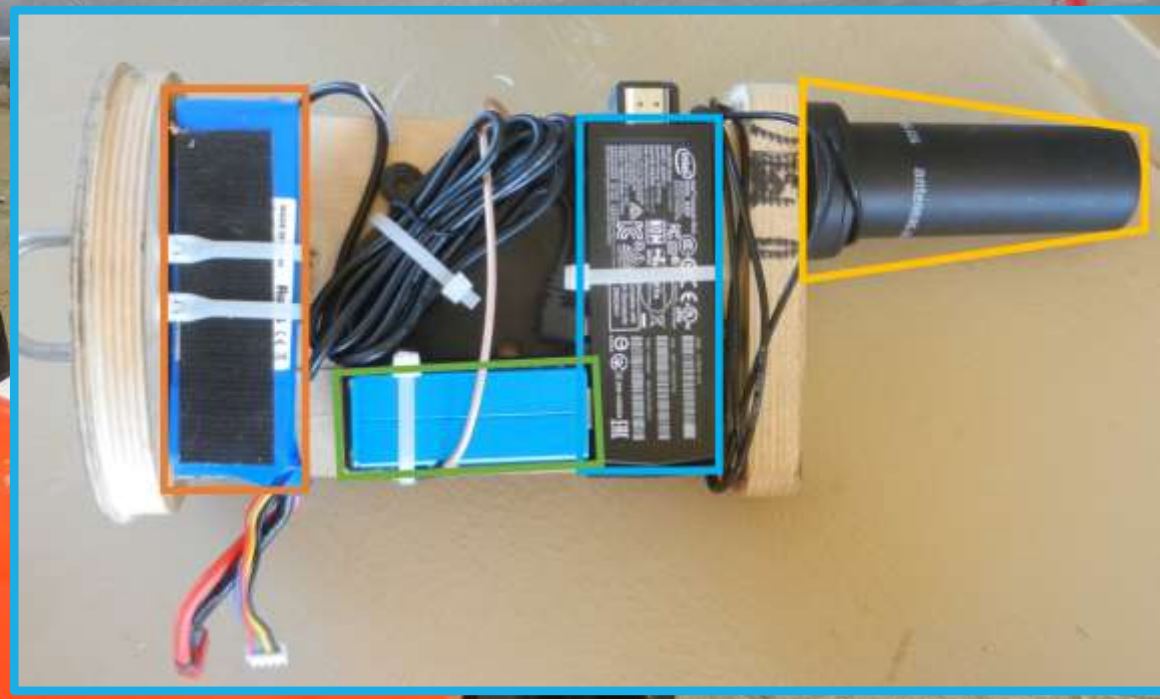
n Bloessl

OTHER APPLICATIONS

GPS ON A HIGH POWERED ROCKET

Most GPS devices are designed to fail if they travel too fast or too high

- COCOM Limit – 1,200 mpg & 59,000 ft.
- Limit imposed by US military
- Limit applied by GPS hardware manufacturers.

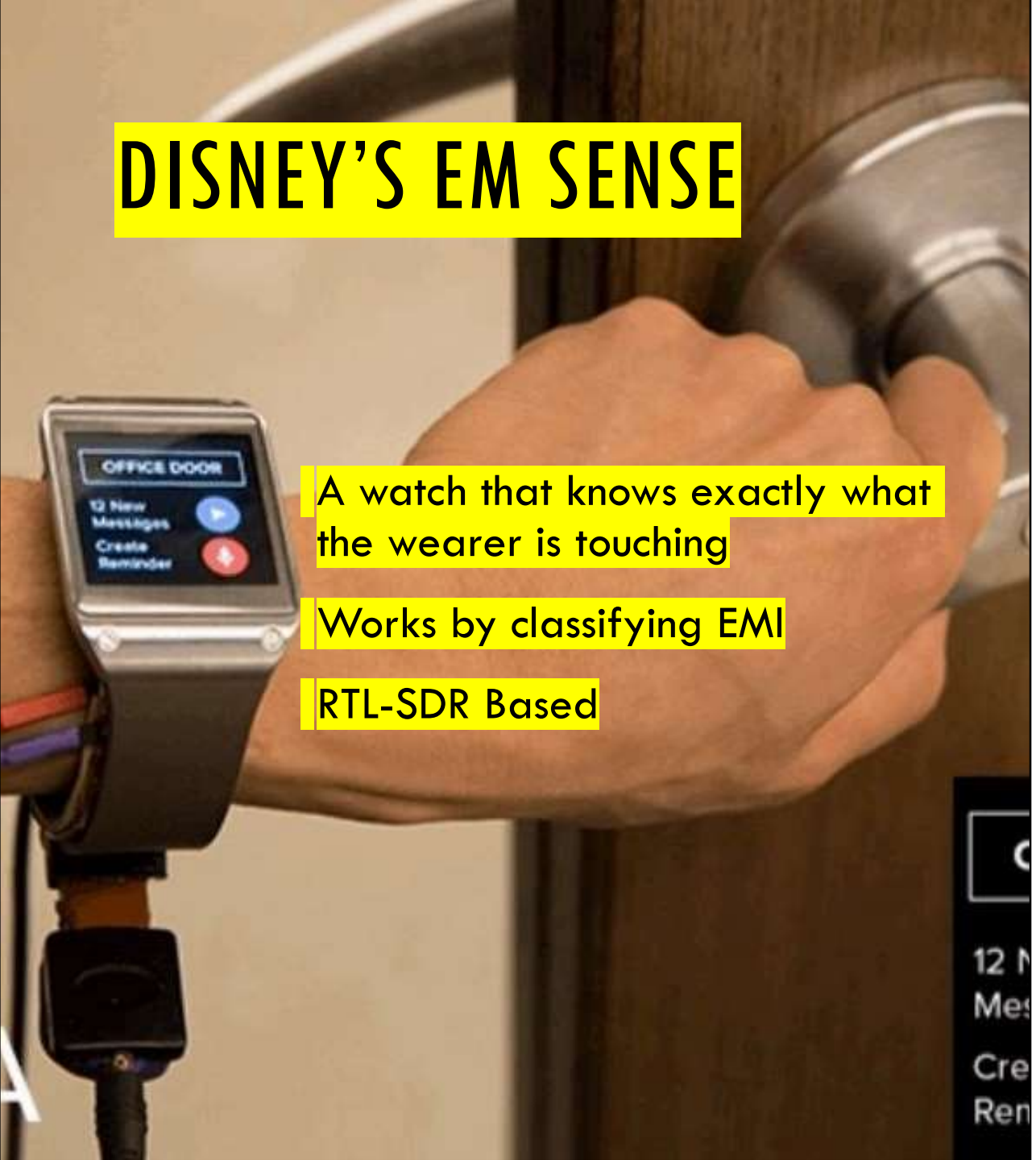


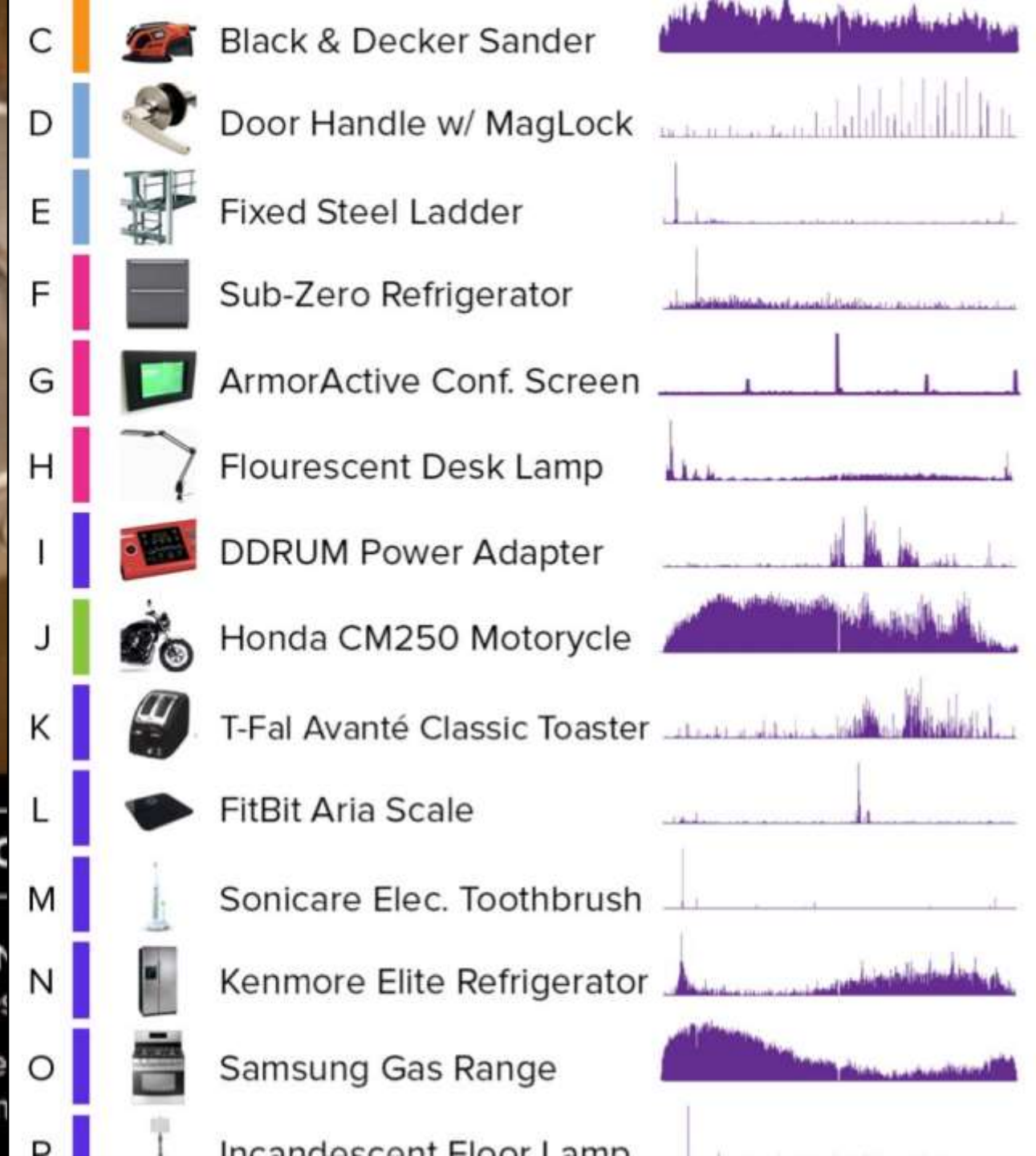
Philip Hahn & Paul Breed building high powered small rockets

- Rocket might be too fast and too high
- Using an RTL-SDR and GNSS-SDR open source software to get position fixes.

DISNEY'S EM SENSE

- A watch that knows exactly what the wearer is touching
- Works by classifying EMI
- RTL-SDR Based





WHAT HAVE I MISSED? LOTS.

- ❑ Listening to the ISS
- ❑ Playstation 3 Reverse Engineering via EMI
- ❑ Reverse Engineering a Heart Defibrillator
- ❑ Decoding VOR
- ❑ ACARS
- ❑ Pagers
- ❑ Defeating IoT Alarms and Car Doors
- ❑ Remote Monitoring
- ❑ Wireless Traffic Analysis
- ❑ Electronic Voice Paranormal Research
- ❑ GOES Weather Satellites
- ❑ Jupiter Noise Bursts
- ❑ Partial Discharge Detection
- ❑ Noise Figure Indicator
- ❑ Receiving Weather balloons
- ❑ Using the RTL-SDR as a VSWR meter
- ❑ Using the RTL-SDR to test RF filters
- ❑ Decoding DAB & DRM
- ❑ Milsatcom Pirates

CONCLUSION

I hope this talk inspired you to try something new with radio

Follow and go through the history of the RTL-SDR.com blog for more interesting projects like this.

Thanks to TAPR for inviting me out to do this talk

Where can I buy RTL-SDR V3 Dongles at Hamvention?

- TAPR booth 5001-5003 Building 5
- R&L Electronics in Building 1
- SDRguys at Booth #7919 in the Flea Market (west end) – also selling Outernet antennas and LNA's

ADDITIONAL SLIDES

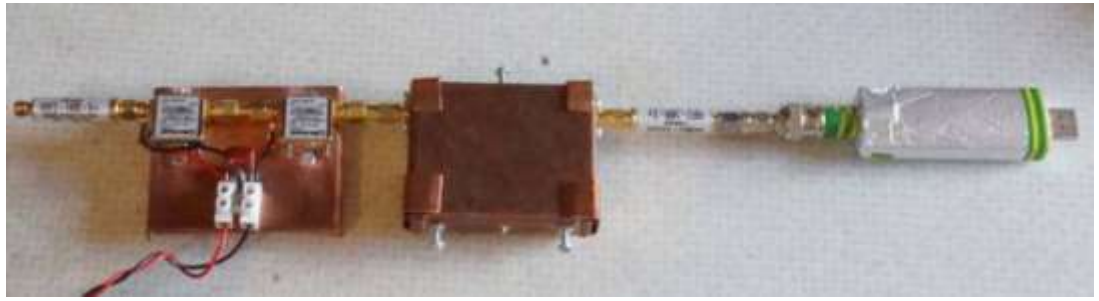
LISTENING TO THE ISS

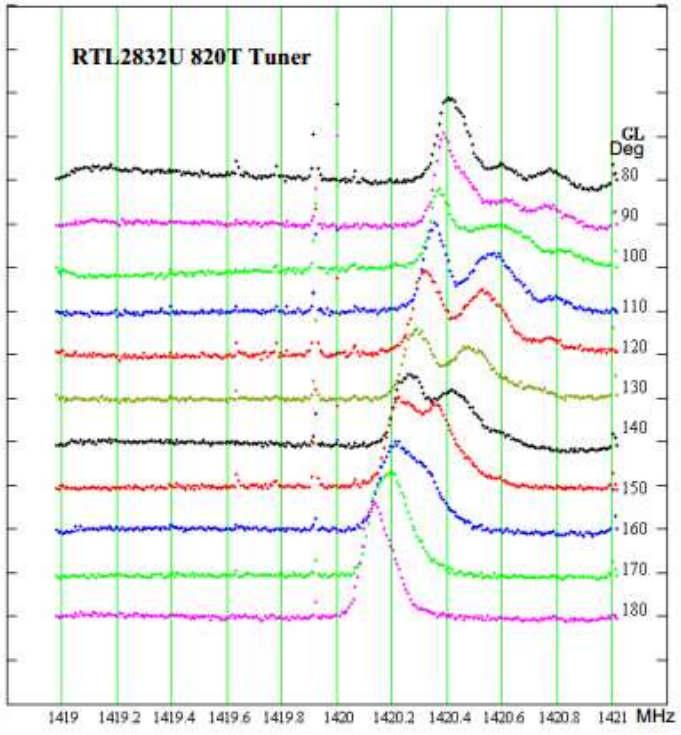
- SSTV Images
- Astronauts talking during spacewalks
- Amateur radio activities
- Digital Amateur TV

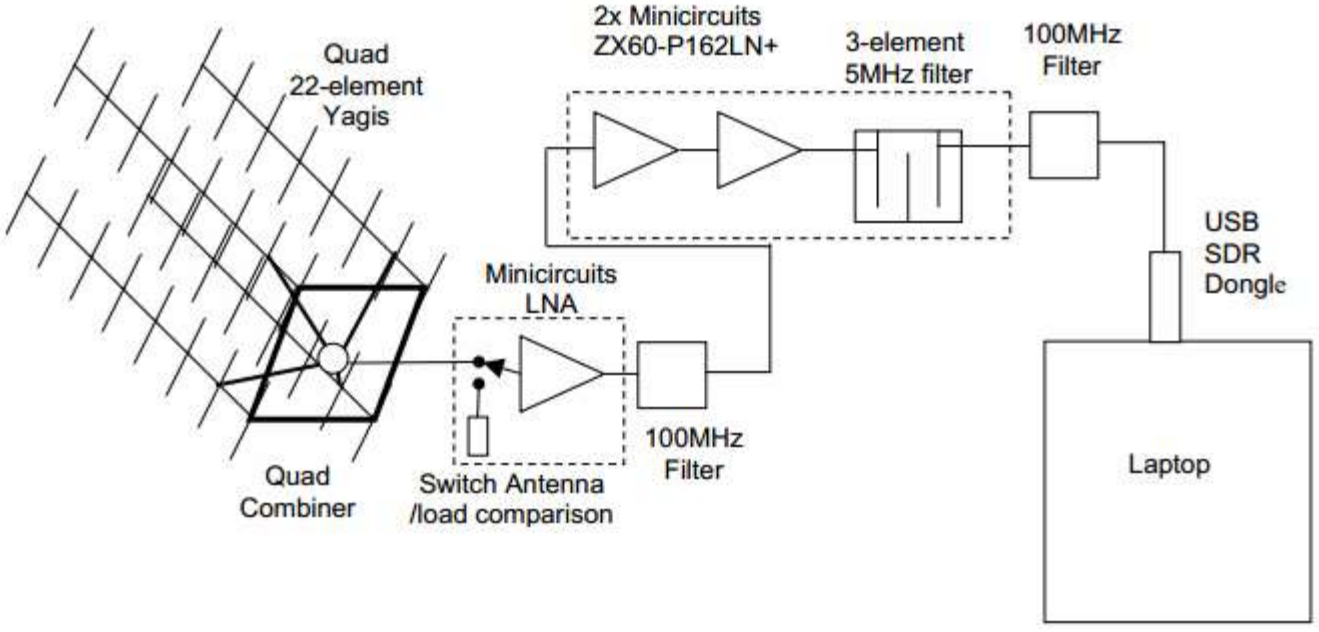
HYDROGEN LINE & GALACTIC PLANE DETECTION

Peter W East

http://www.y1pwe.co.uk/RAProgs/index.html

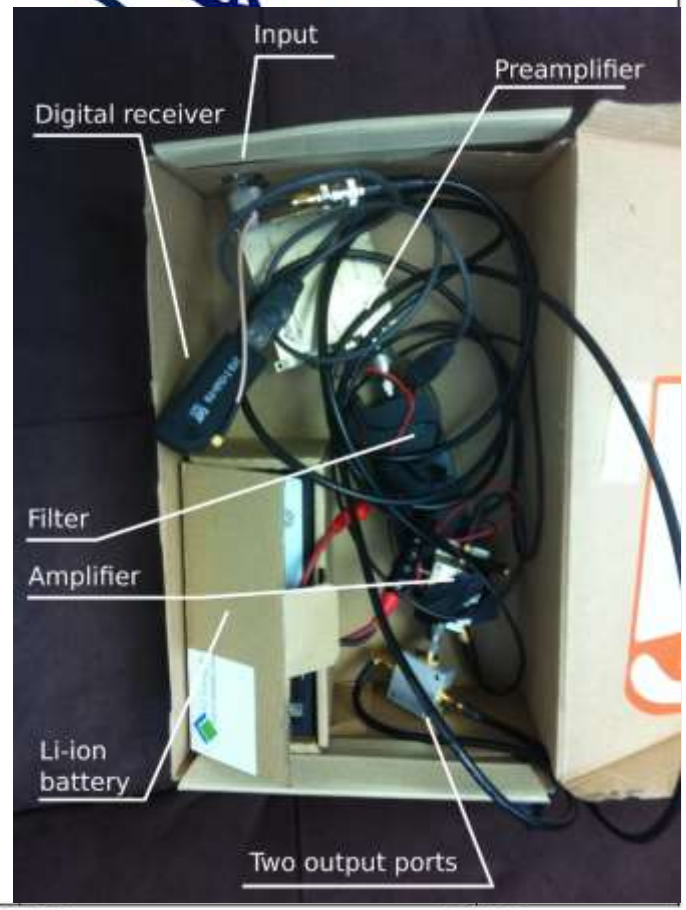






QRM/NOISE DETECTION AND LOCATING

- MIT Haystack Observatory - Juha Vierinen
- Sudden QRM at 440 MHz – their Radar band
- RTL-SDR solution to help find hotspots
- Together with Yagi measurements found the hotspot
- A faulty FSK telemetry link on a nearby FM tower



PLAYSTATION 3 REVERSE ENGINEERING ATTEMPT

Hackers want to ‘Jailbreak’ gaming consoles

- Allows custom software to be installed
- Custom games etc.

Connect RTL-SDR antenna input between chassis and real ground (ground rods)

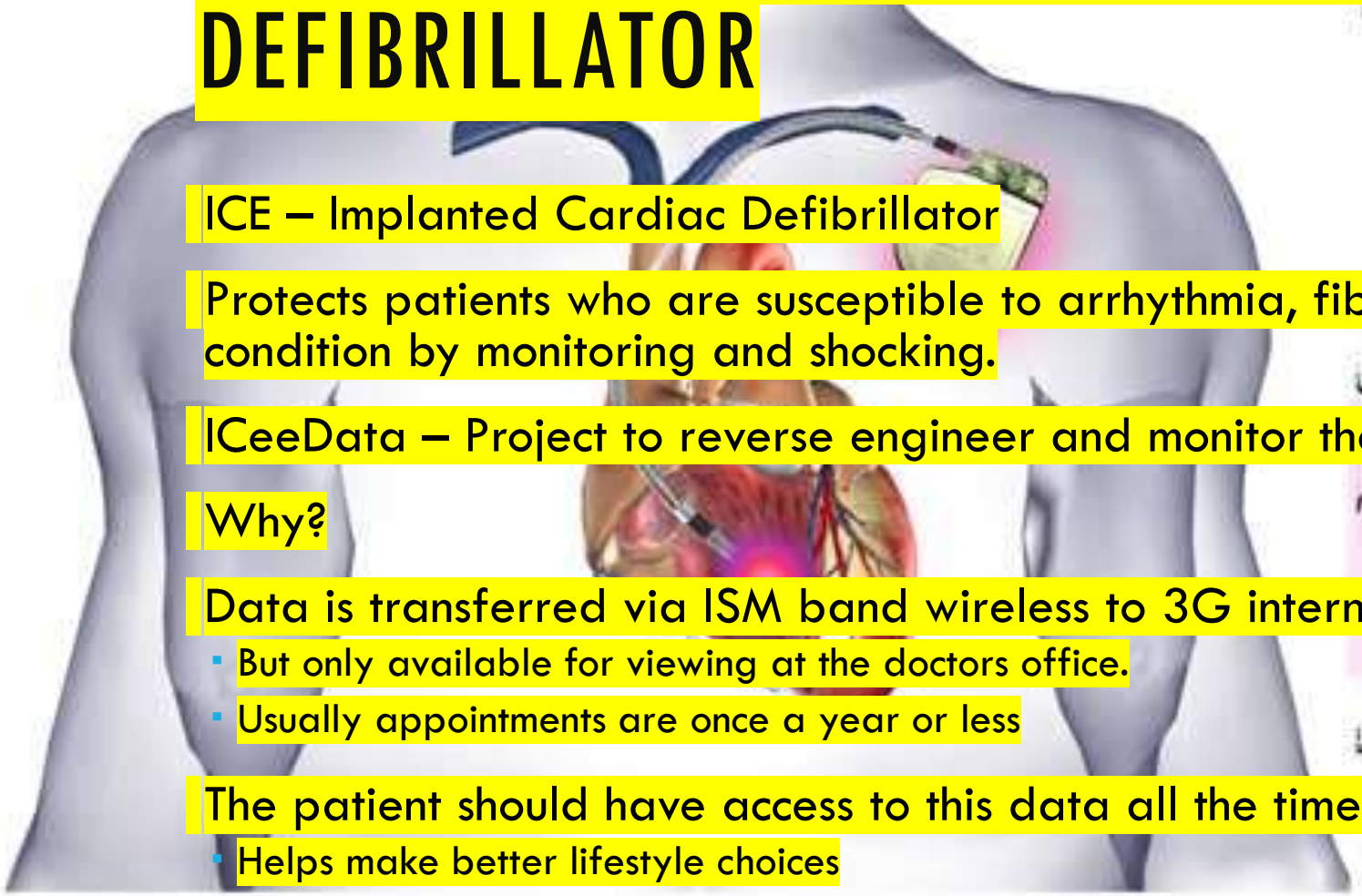
RTL-SDR receives CPU noise

Can try to decode CPU instructions from the noise

Never got very far in the reverse engineering process

- Lawsuit fears

REVERSE ENGINEERING AN IMPLANTED CARDIAC DEFIBRILLATOR



ICE – Implanted Cardiac Defibrillator

Protects patients who are susceptible to arrhythmia, fibrillations and abnormal heart condition by monitoring and shocking.

ICeeData – Project to reverse engineer and monitor the wireless telemetry data

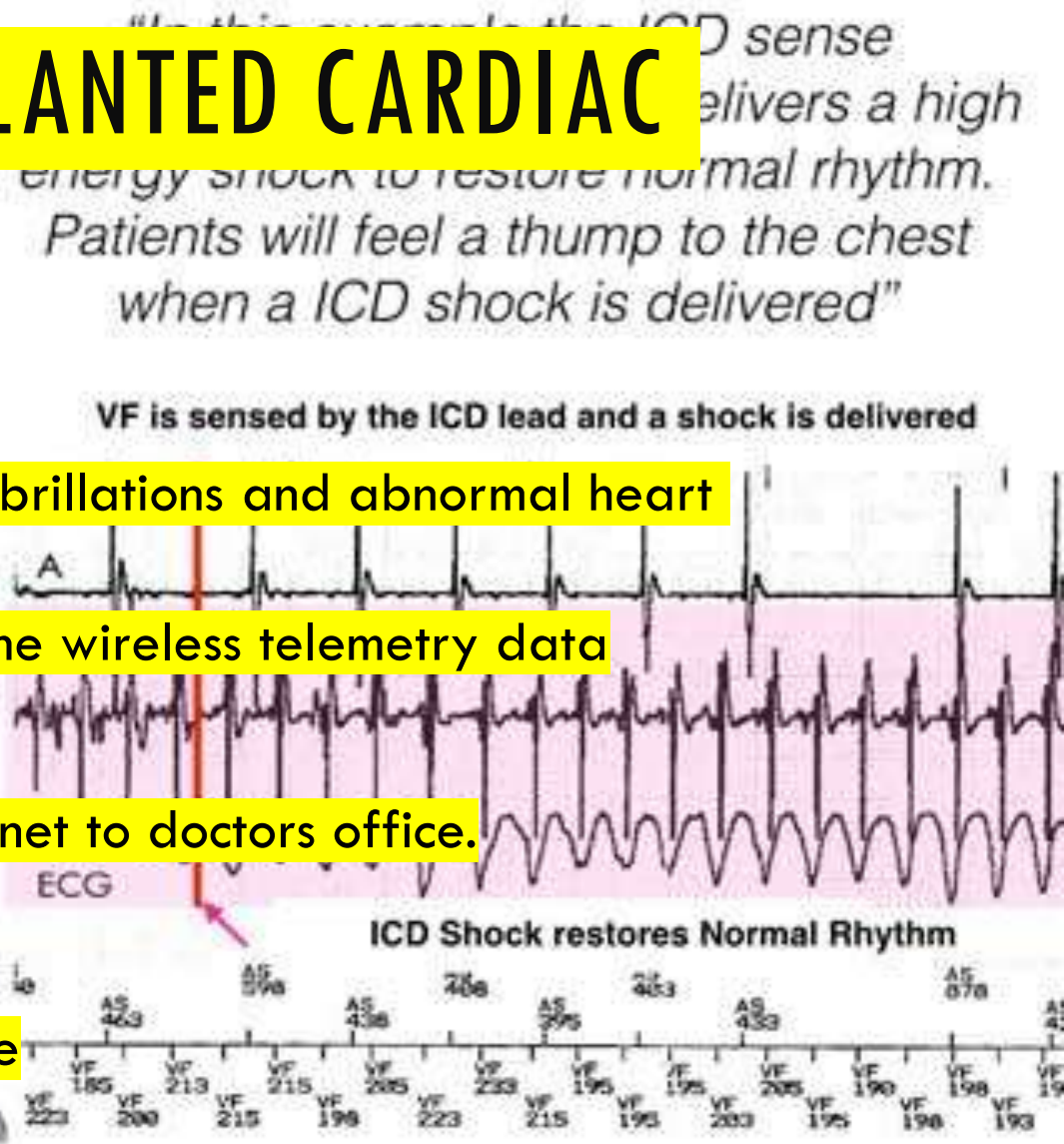
Why?

Data is transferred via ISM band wireless to 3G internet to doctors office.

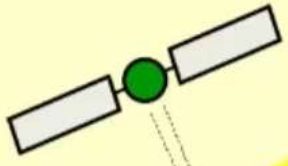
- But only available for viewing at the doctors office.
- Usually appointments are once a year or less

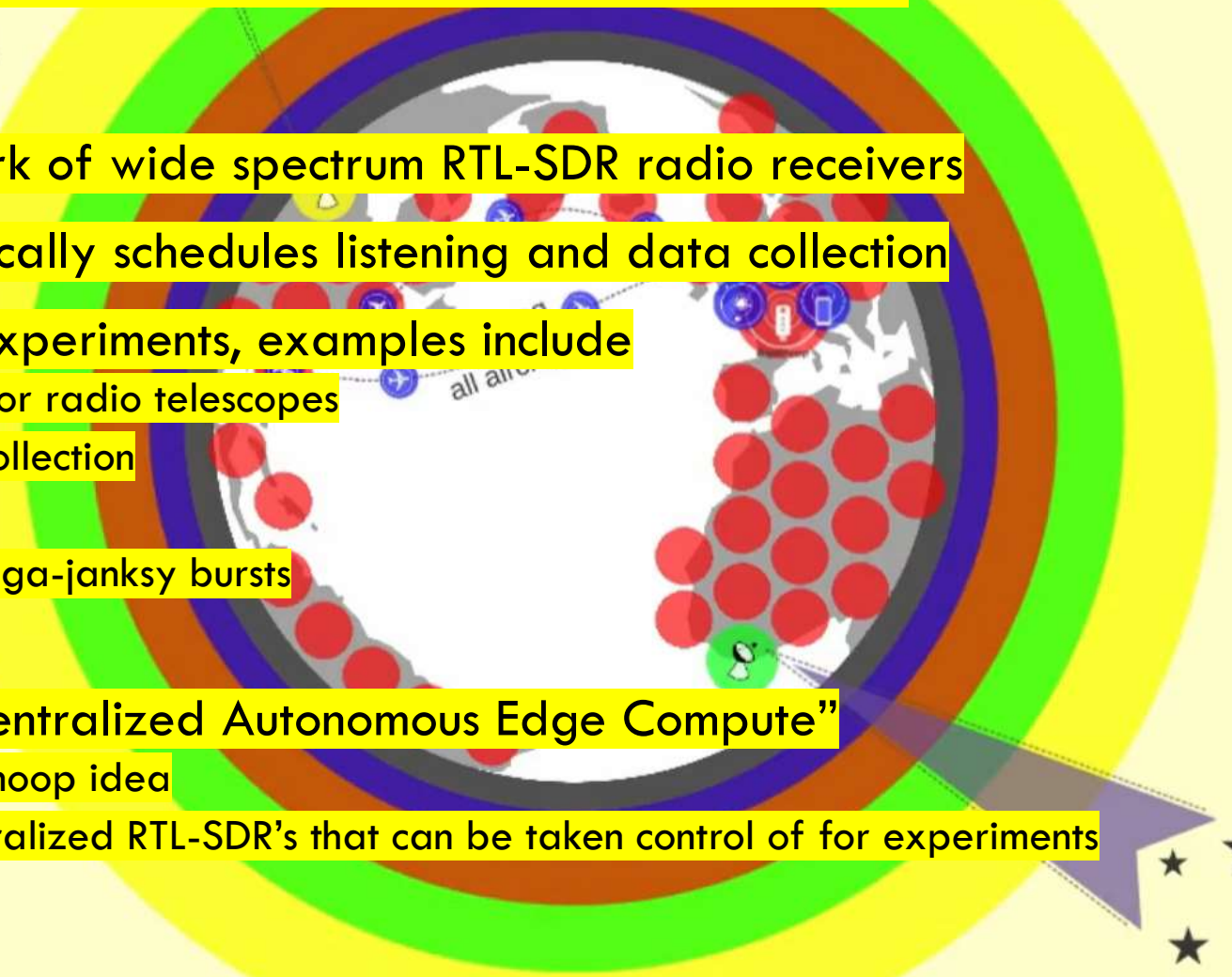
The patient should have access to this data all the time

- Helps make better lifestyle choices



GLOBAL NETWORKED MONITORING





Bigwhoop – network of wide spectrum RTL-SDR radio receivers

Network automatically schedules listening and data collection

Focus on science experiments, examples include

- Finding quiet spots for radio telescopes
- LEO satellite data collection
- Spectrum monitoring
- Radio astronomy: Giga-janksy bursts

IBM “Horizon Decentralized Autonomous Edge Compute”

- Similar to the big whoop idea
- Hundreds of decentralized RTL-SDR’s that can be taken control of for experiments

...or finding sweet spots for radio telescopes.

DECODING VOR

VOR – VHF Omnidirectional Range

- An old method of air navigation
- Still heavily used but slowly being replaced by GPS

Gives you the angle of the aircraft from the transmitter

Works by sending out an omnidirectional master signal, and a highly directional second signal.

The directional signal rotates 360 degrees with an antenna array.

hpux735 took his RTL-SDR on a flight and recorded VOR signals

Later used his GNU Radio VOR decoder to decode the aircraft position

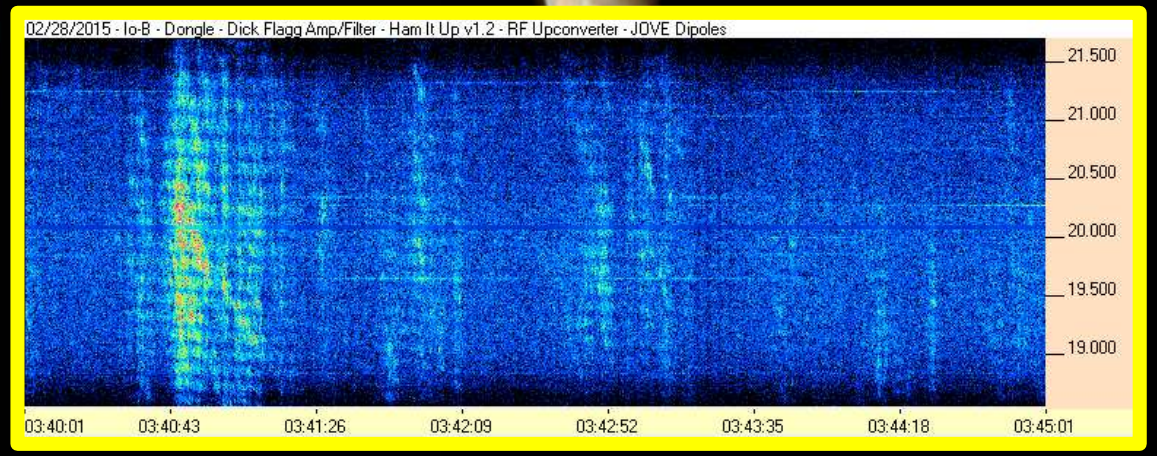
JUPITER NOISE BURSTS

Listening to bursts of noise between 20 – 40 MHz originating from the planet Jupiter

Creates “radio noise storms” through a complex orbital relationship between Jupiter and its volcanic moon Io.

What do you need to receive Jupiter noise?

- Antenna: A simple dipole tuned to around 20 MHz will work
- Filter + LNA
- Any radio like an RTL-SDR



TPMS TIRE DATA

TPMS - Tire Pressure Monitoring System

Wirelessly transmits tyre pressure data to a dashboard in the car

- Place one sensor per tyre

Can easily receive and decode the data with an RTL-SDR

Security Issue?

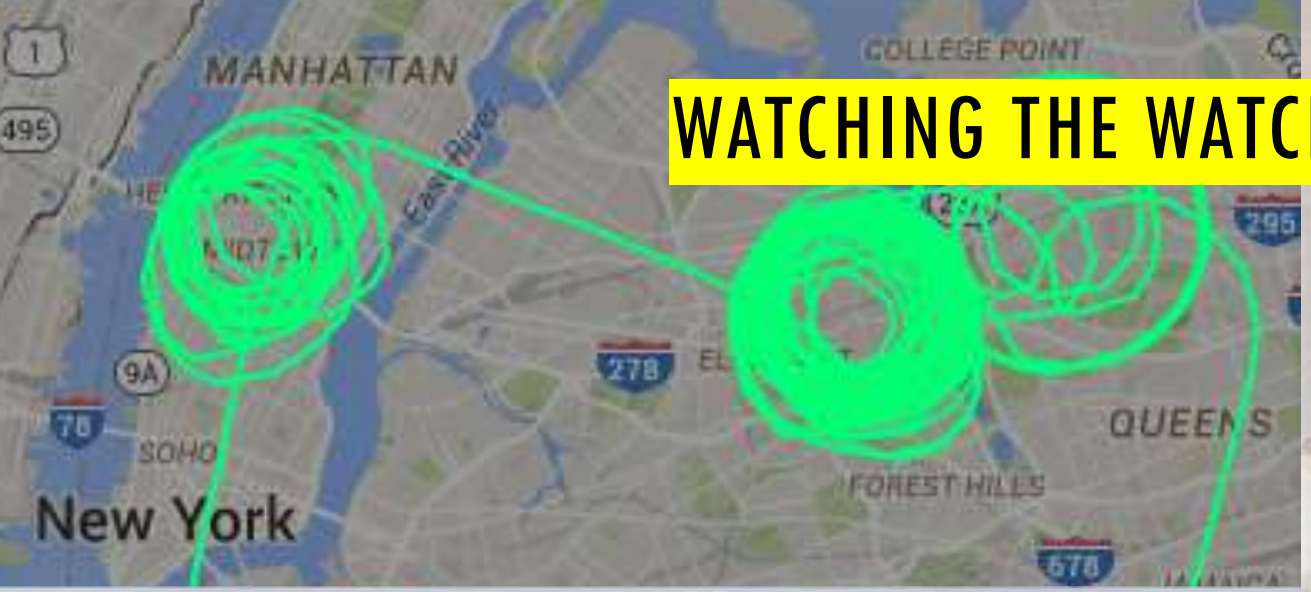
Each sensor has a unique ID

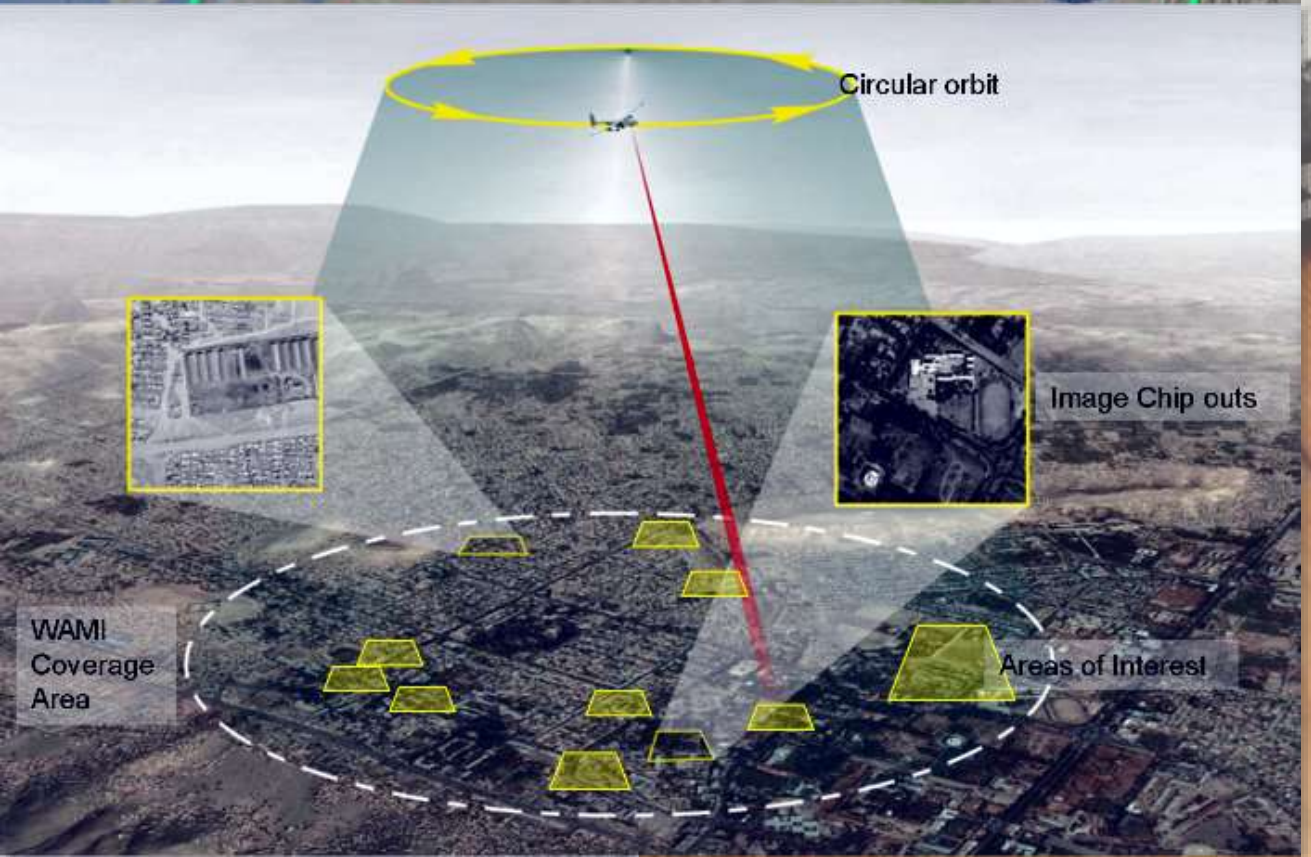
- Could potentially track vehicles across town

LIVE COCKPIT FROM ADS-B DATA

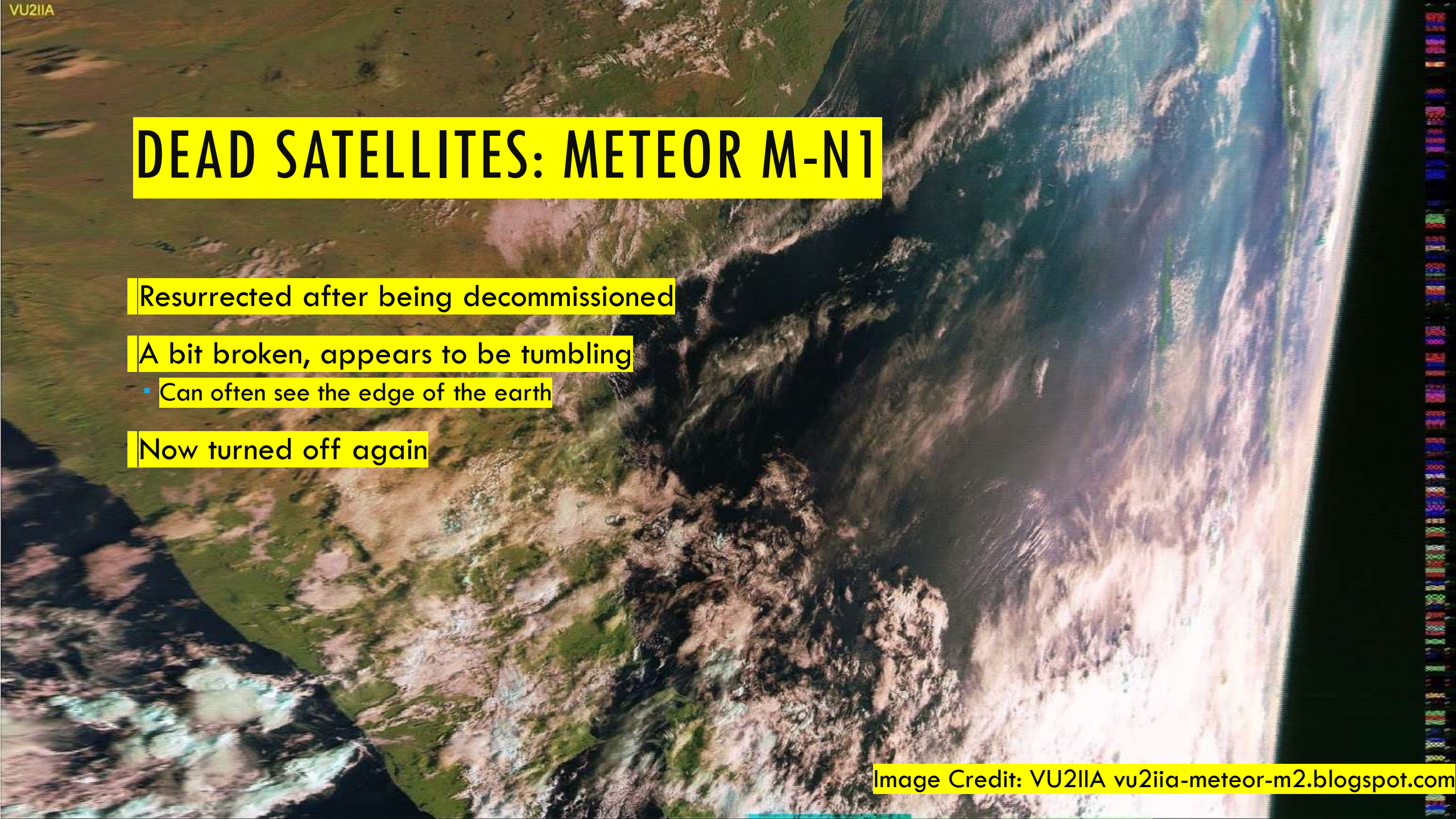
- Tomvd's RTL1090XHSI
- Use live ADS-B data to create an authentic cockpit experience
- Based on flight simulator software
- Be careful when using on an actual aircraft
  - Don't panic people

WATCHING THE WATCHMEN WITH ADS-B





- Persistent Wide-Area Surveillance
  - Persistent Surveillance Systems in Dayton, OH
- IMSI Catchers
  - Allows authorities to listen to cellphones
- John Wiseman @lemonodor notices suspicious aircraft circling for days after the Baltimore riots.
  - He has 6 months of ADS-B logs from his RTL-SDR
- Searching for the squawk codes he finds several similar flights in his logs.
- All registered to generically named fake companies.
- FBI later confirms that they are their aircraft
- Most likely persistent wide-area surveillance



DEAD SATELLITES: METEOR M-N1

- Resurrected after being decommissioned
- A bit broken, appears to be tumbling
  - Can often see the edge of the earth
- Now turned off again

Image Credit: VU2IIA vu2iia-meteor-m2.blogspot.com

REDESIGNED RTL-SDR V3

Problems with “Generic” dongles

1. Drifting oscillator (unstable frequency)
2. No shielding
3. Many spurs
4. Problems with L-band reception
5. Uncommon MCX RF connector

RTL-SDR.com V3 fixes and added features

1. TCXO Oscillator
2. Metal case shielding
3. Redesigned PCB, and additional noise filtering
4. Thermal pad to metal case heat sink
5. SMA connector
6. Bias tee
7. HF reception via direct sampling

DECODING WEATHER BALLOONS

- Twice daily weather balloon launches in many local areas
- Different countries use different radio protocols and frequencies
- COAA SondeMonitor decodes most
- Transmits weather data and GPS location
- Some people chase and collect them
- Amateur radio balloons are quite similar

MEASURING FILTER CHARACTERISTICS AND ANTENNA VSWR

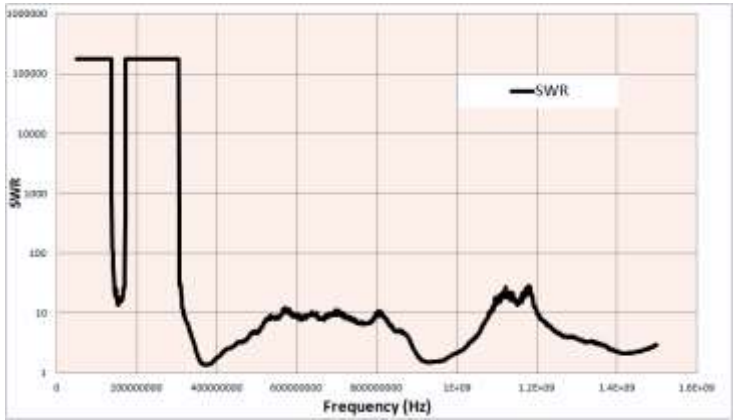
RTL-SDR as a network analyser

- Measure filter characteristics
- Measure coax stubs
- Measure antenna VSWR

Not totally accurate, but gives you a good enough reading.

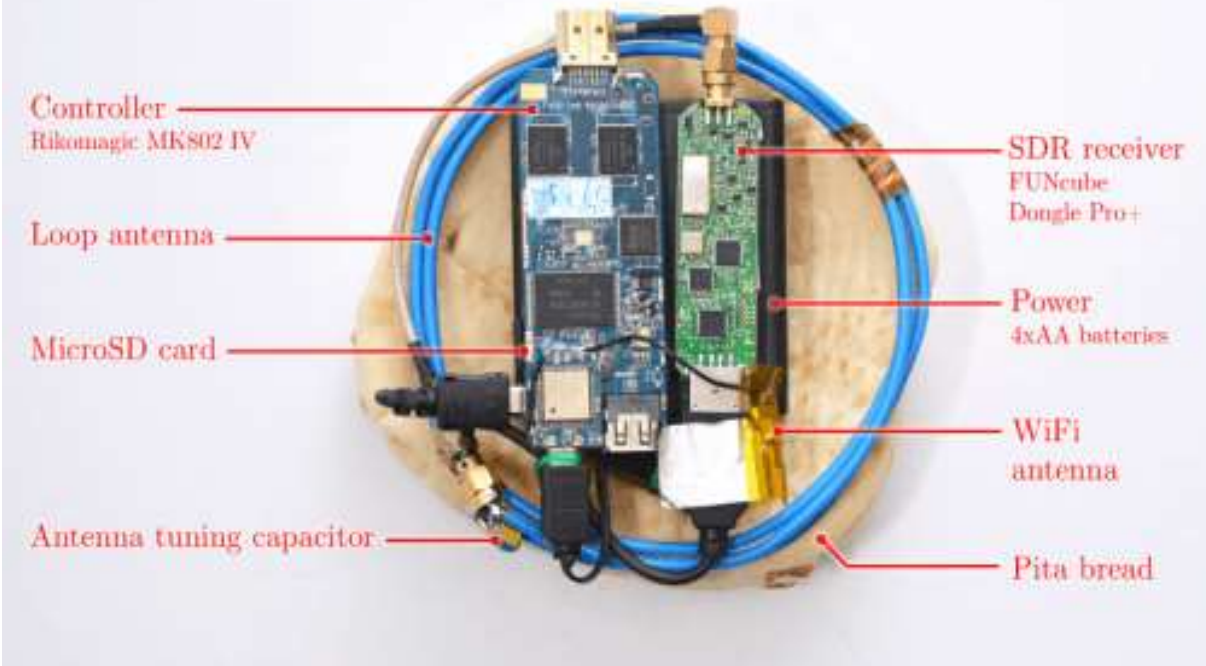
What do you need:

- RTL-SDR
- Wideband noise source
- Directional coupler



STEALING ENCRYPTION KEYS FROM PCS

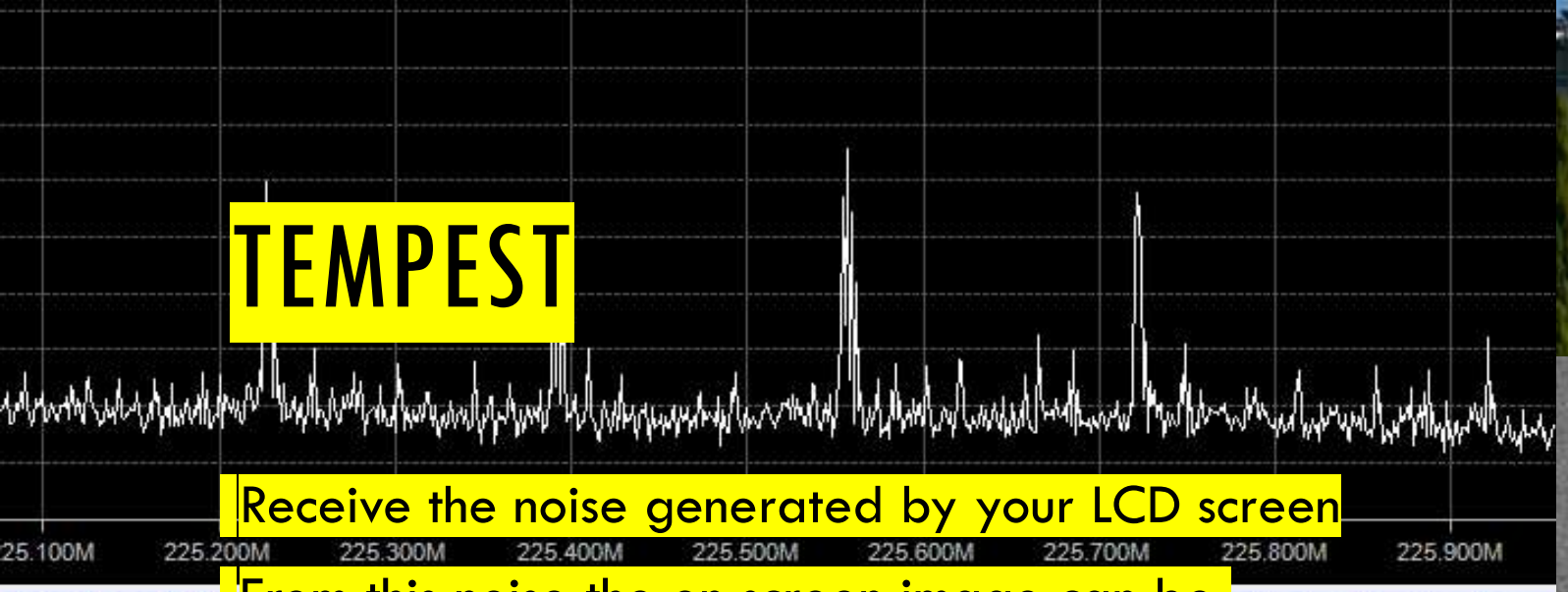
- Every computer emits some RFI
- The RFI frequency changes depending on what the computer is doing
- By monitoring the RFI assembly programming instructions can be determined
- Used to extract encryption keys from a PC
- Any radio can be used
  - They even demonstrate using a pocket AM radio



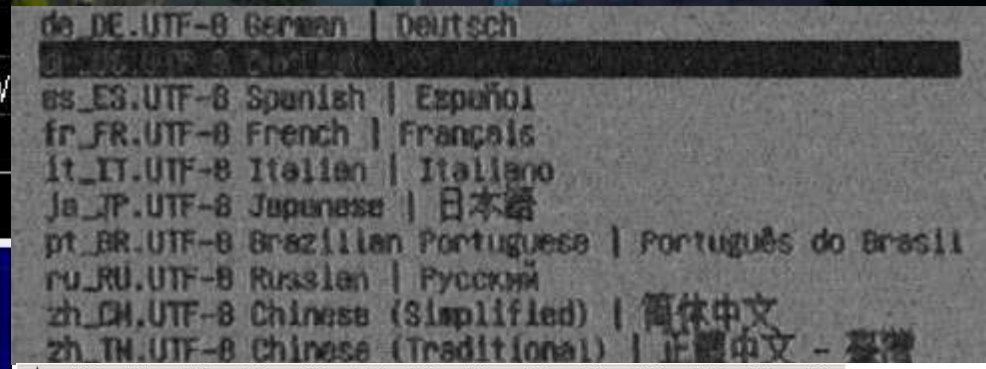
HOW TO RECEIVE THESE WEATHER SATELLITES

- They are in “low earth orbit”
  - Close to earth, but orbit quite quickly
  - Each pass will be about 10 minutes
- Need a satellite antenna (beams radiation pattern towards sky)
  - QFH
  - Turnstile
  - V-Dipole
- Use software like Orbitron to track the satellites

TEMPEST



- Receive the noise generated by your LCD screen
- From this noise the on screen image can be recovered
- RTL-SDR Software: TempestSDR
- Example: My LCD emits RFI at ~225 MHz. Tones change depending what is on the screen
- Use SDR to steal encryption keys from a PC
  - Get Assembly code instructions
- Reverse engineer a Playstation



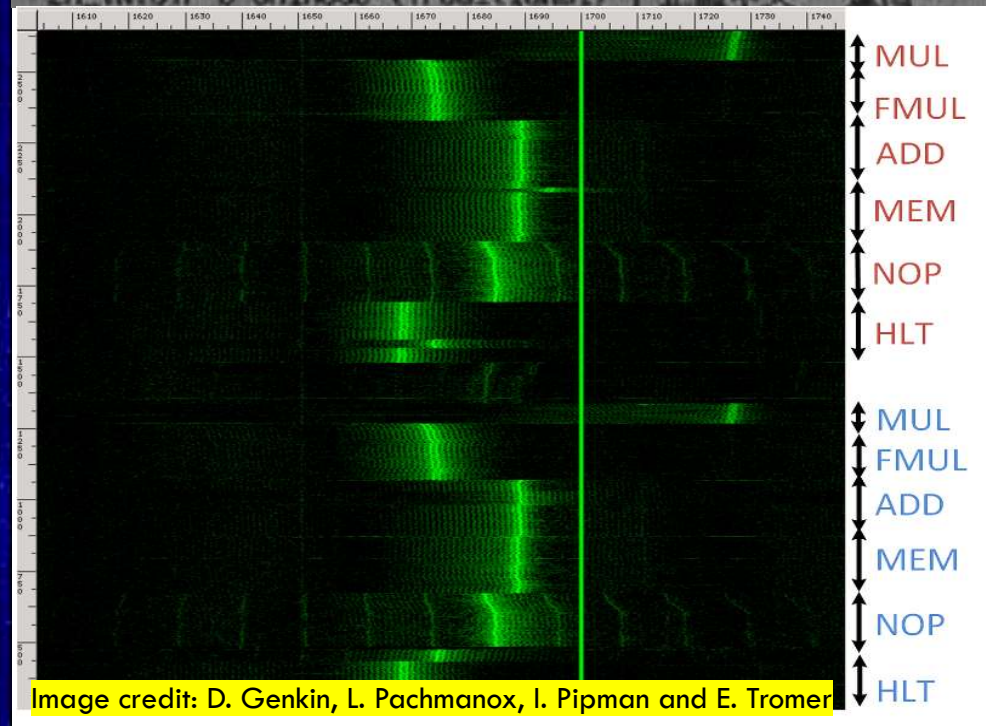
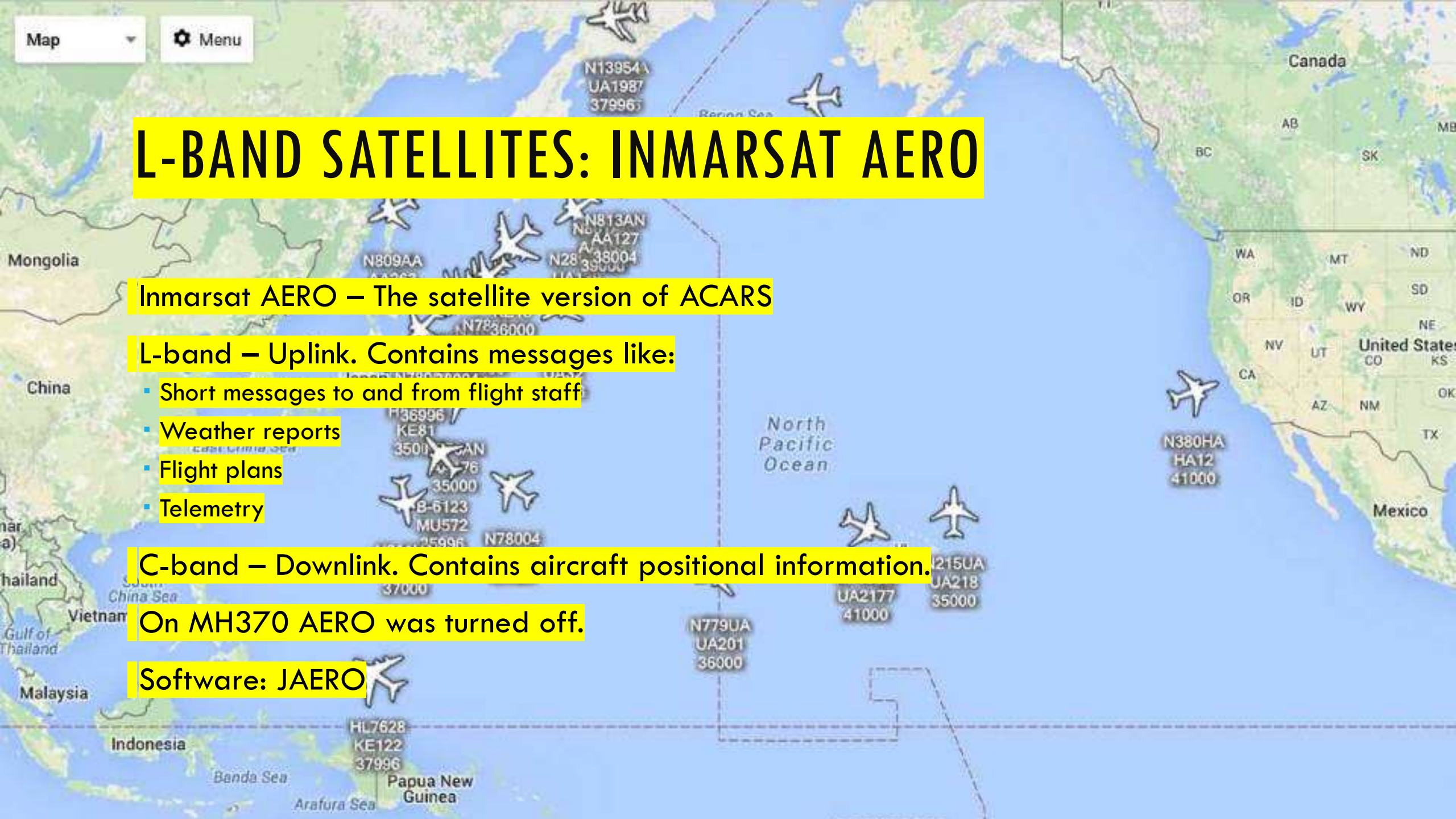


Image credit: D. Genkin, L. Pachmanox, I. Pipman and E. Tromer



L-BAND SATELLITES: INMARSAT AERO

Inmarsat AERO – The satellite version of ACARS

L-band – Uplink. Contains messages like:

- Short messages to and from flight staff
- Weather reports
- Flight plans
- Telemetry

C-band – Downlink. Contains aircraft positional information.

On MH370 AERO was turned off.

Software: JAERO