

LE MONDE À FAIBLE COÛT

LOGICIEL RADIO DEFINIE

Par Carl Laufer

Qui suis-je.

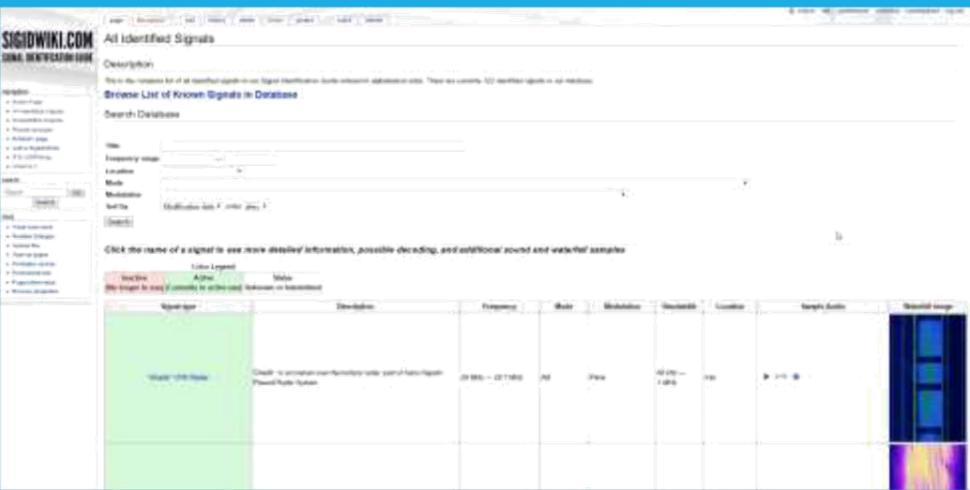
J'ai exécuté le blog RTL-SDR.com depuis 2013

J'ai collecté les histoires relatives à la radio ultra bon marché

J'ai redessiné le dongle RTL-SDR pour un SDR performances amélioré.

J'ai démarré sigidwiki.com, une collection de signaux

www.rtl-sdr.com



Un logiciel RX très bon marché définit la radio en fonction de la radio définie par le logiciel RX très bon marché basée sur le chipset RTL2832U.

Radio définie par le logiciel?

Fondamentalement, un tuner et un ADC.

Tout démoduler est fait par le logiciel.

A l'origine (et est toujours) un tuner TV DVB-T

Produite en gros en Chine - très bon marché.

Les pirates informatiques ont trouvé la fonction SDR.

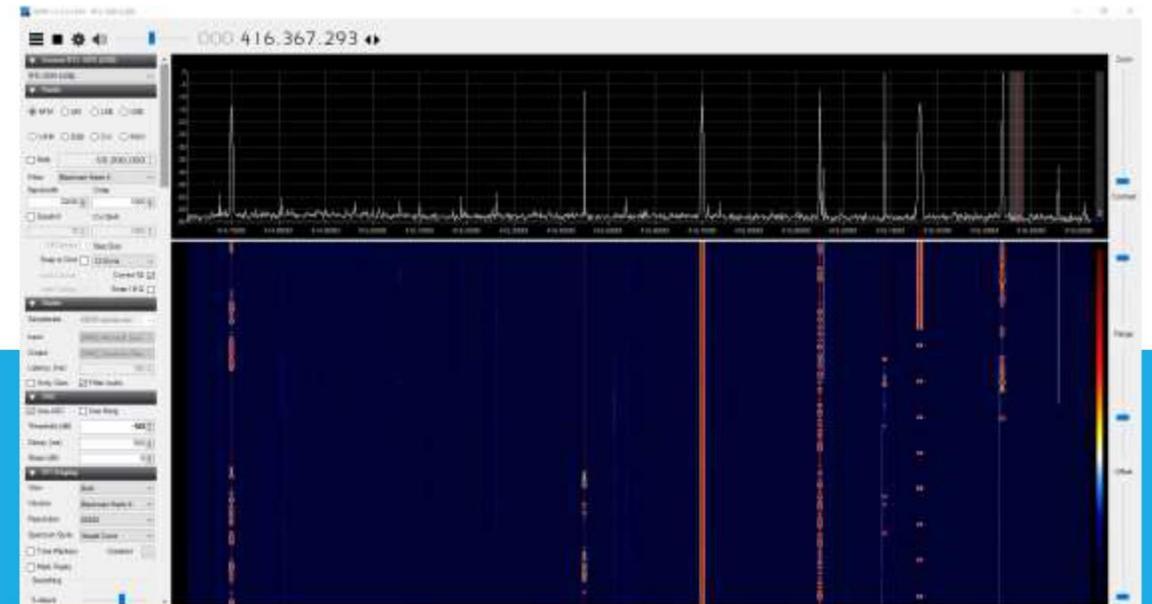
À l'origine conçu pour la réception radio FM

Ils ont écrit des drivers personnalisés pour étendre sa gamme de fréquences Soudain, c'est un récepteur extrêmement polyvalent.

Peut recevoir / démoduler / décoder presque n'importe quoi de 24 - 1,8 GHz pour 10 USD.

Ouvert un tout nouveau monde d'expérimentation.

Nouveau (et vieux) sang revenant à la scène radio.



Il y a beaucoup d'applications, commençons!

DE CE QUI SUIVRAIT-IL?

Une vue d'ensemble ou une
«Revue de la littérature»
Sur les applications intéressantes pour le
RTL-SDR.

Éviter le scanner "commun"

Les applications, parleront des plus
étranges et des créneaux.

Il y a beaucoup d'applications,
commençons!

APPLICATIONS DE
SCANNER COMMUN
POUR UN RTL-SDR.

Radio amateur

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

Communication analogique EMS.

Communications EMS numériques,
P25, DMR, TETRA.

Trunked Radio.

Le contrôle du trafic aérien.

SUIVI DES AÉRONEFS ET DES BATEAUX



ADS-B: SUIVI DES AVIONS

- Surveillance dépendante automatique - diffusion

- Mode-S

- 1090 MHz

- ADS-B Diffuse des paquets contenant des informations de position



Map Satellite

C81CF8

QFA136

New Zealand

Type:
Time Tracked: 15:24
From: NZAA Auckland Intl, New Zealand
To: YMML Melbourne Intl, Australia
Above: Position lookup disabled
Toggle position lookup

Climbing through 8938 metres at 429 metres/min, ground speed 676 km/h, heading west 250.5°, 132.59 km southwest of here at 244.2°. Squawking 0243.

Disable auto-select :: Select closest :: Hide selection :: Page help

Date Report :: Registration Report :: ICAO Report
Show options

Tracking 6 aircraft

Reg.	ICAO	Callsign	Type	Alt.	Squawk	Pause Speed
●	7C683C	JST239		10653	1067	971
●	89619A	UAE434		11278		103
●	C8178C	ANZ823		10973	0240	674
●	3A2644	ACI410A		9091	4422	820
●	C81CF8	QFA136		8938	0243	676
●	C815A1			4054	5723	

Powered by Virtual Radar Server

ADSB# v1.0.9.1

Stop Port 47806

Share with ADSBHub Host sdrsharp.com

Decoder

Confidence	Timeout (sec)	Frames/sec
3	120	5

UTILISATIONS DONNÉES ADS-B DE RTL-SDRS?

Sites Web de suivi des vols commerciaux
[FlightAware.com](https://www.flightaware.com)

[FlightRadar24.com](https://www.flightradar24.com)

Pilotes de navigation

UTC 01:46



RECEPTION ADS-B STATION

RTL-SDR (10 \$ - 20 \$)

Filtre (20 \$)

Raspberry Pi (35 \$)

Antenne (30 \$)

Coût total ~ 100 \$

978 MHz UAT

Transcepteur d'accès universel (UAT)

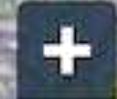
Utilisé principalement aux États-Unis

Semblable à ADS-B, mais principalement utilisé par les petits avions

Fournit des services supplémentaires
Données météorologiques en direct

Décoder avec dump978

Ou plusieurs applications Android



35.91°N / 80.71°W

35.05°N / 80.01°W

35.30°N / 79.60°W

STRATUX

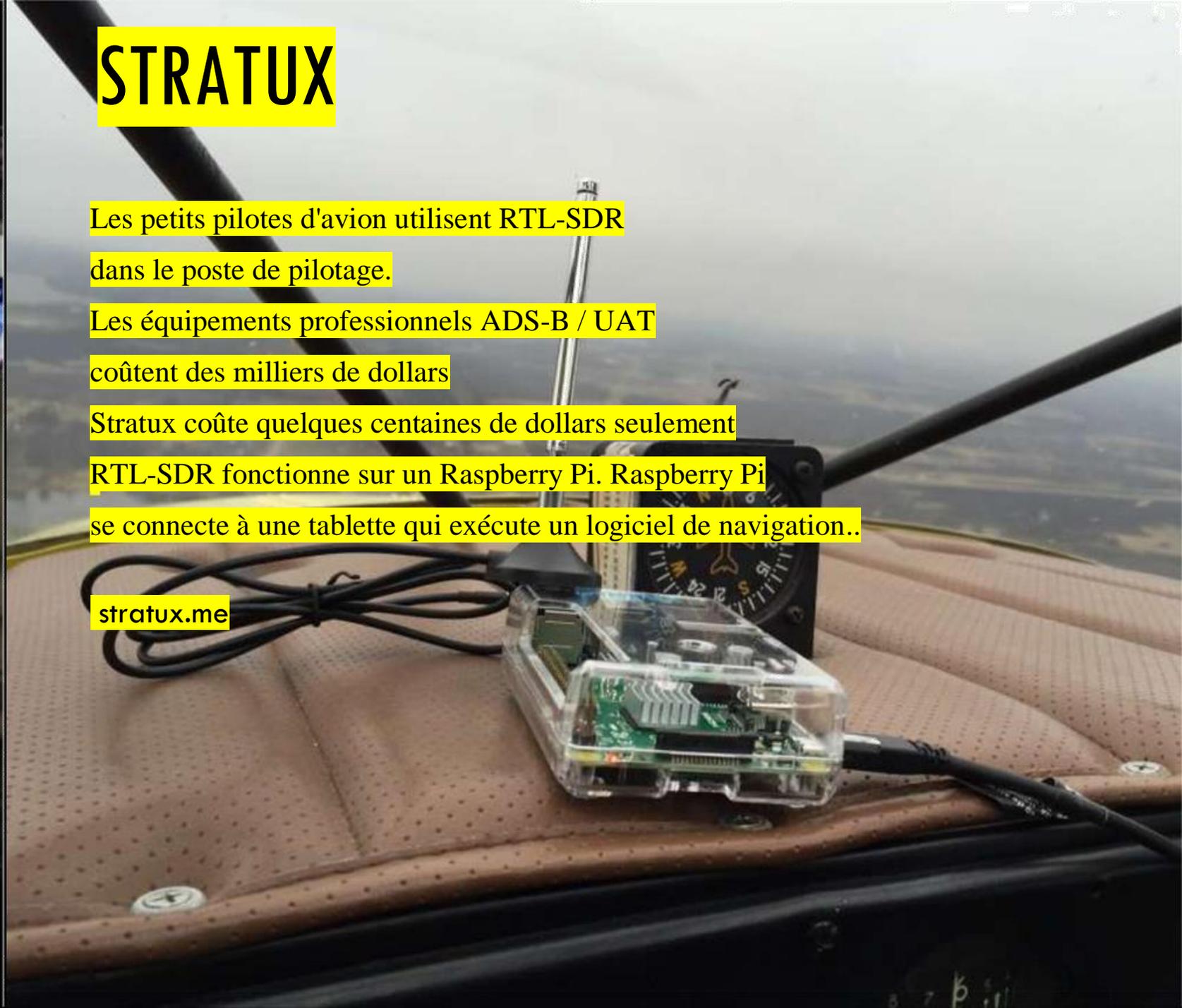
Les petits pilotes d'avion utilisent RTL-SDR dans le poste de pilotage.

Les équipements professionnels ADS-B / UAT coûtent des milliers de dollars

Stratux coûte quelques centaines de dollars seulement

RTL-SDR fonctionne sur un Raspberry Pi. Raspberry Pi se connecte à une tablette qui exécute un logiciel de navigation..

stratux.me



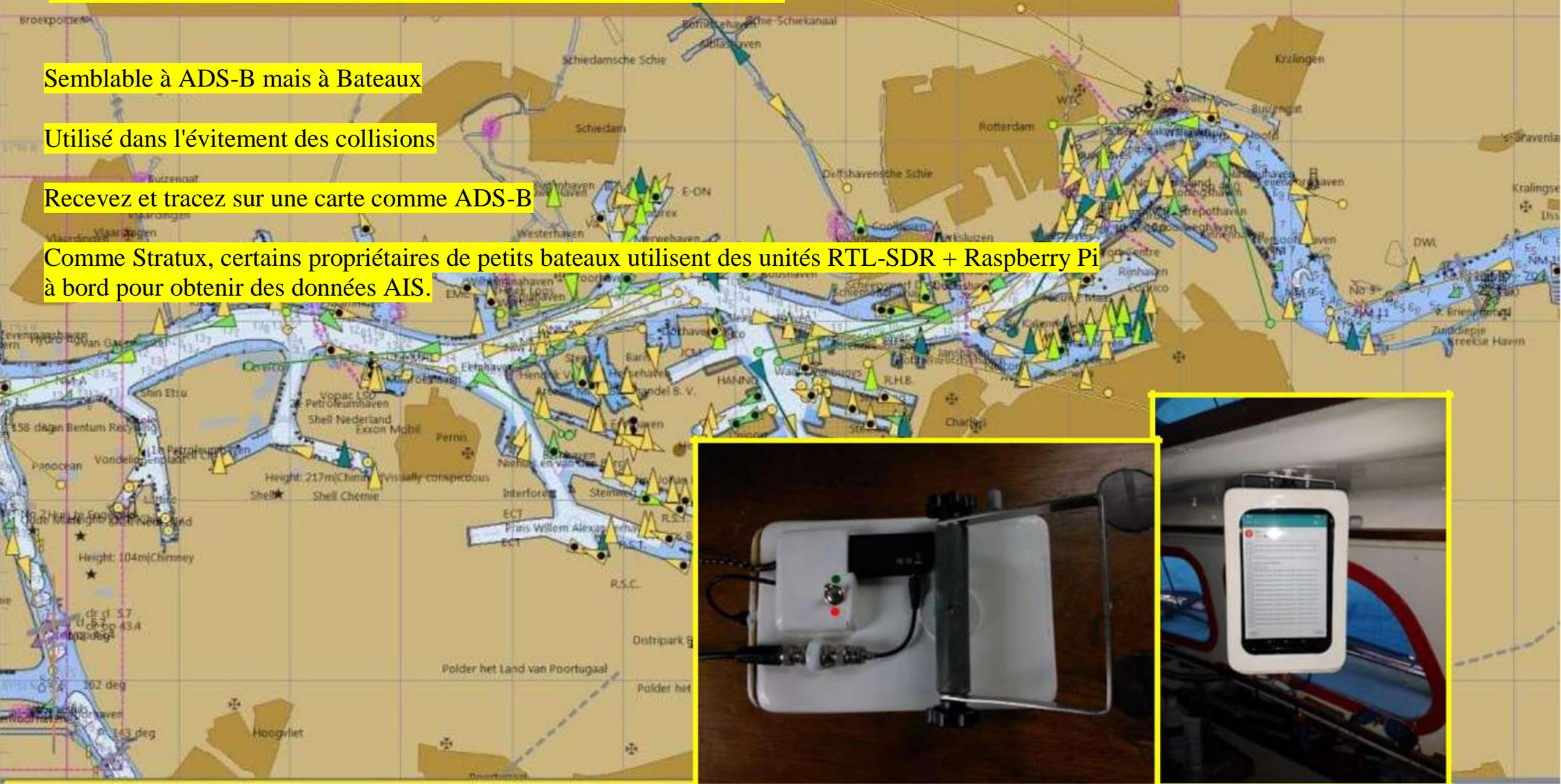
AUTOMATIC IDENTIFICATION SYSTEM (AIS)

Semblable à ADS-B mais à Bateaux

Utilisé dans l'évitement des collisions

Recevez et tracez sur une carte comme ADS-B

Comme Stratux, certains propriétaires de petits bateaux utilisent des unités RTL-SDR + Raspberry Pi à bord pour obtenir des données AIS.



LEO SATELLITES



NOAA SATELLITES MÉTÉO

Recevez des images météorologiques en direct

Trois satellites actifs

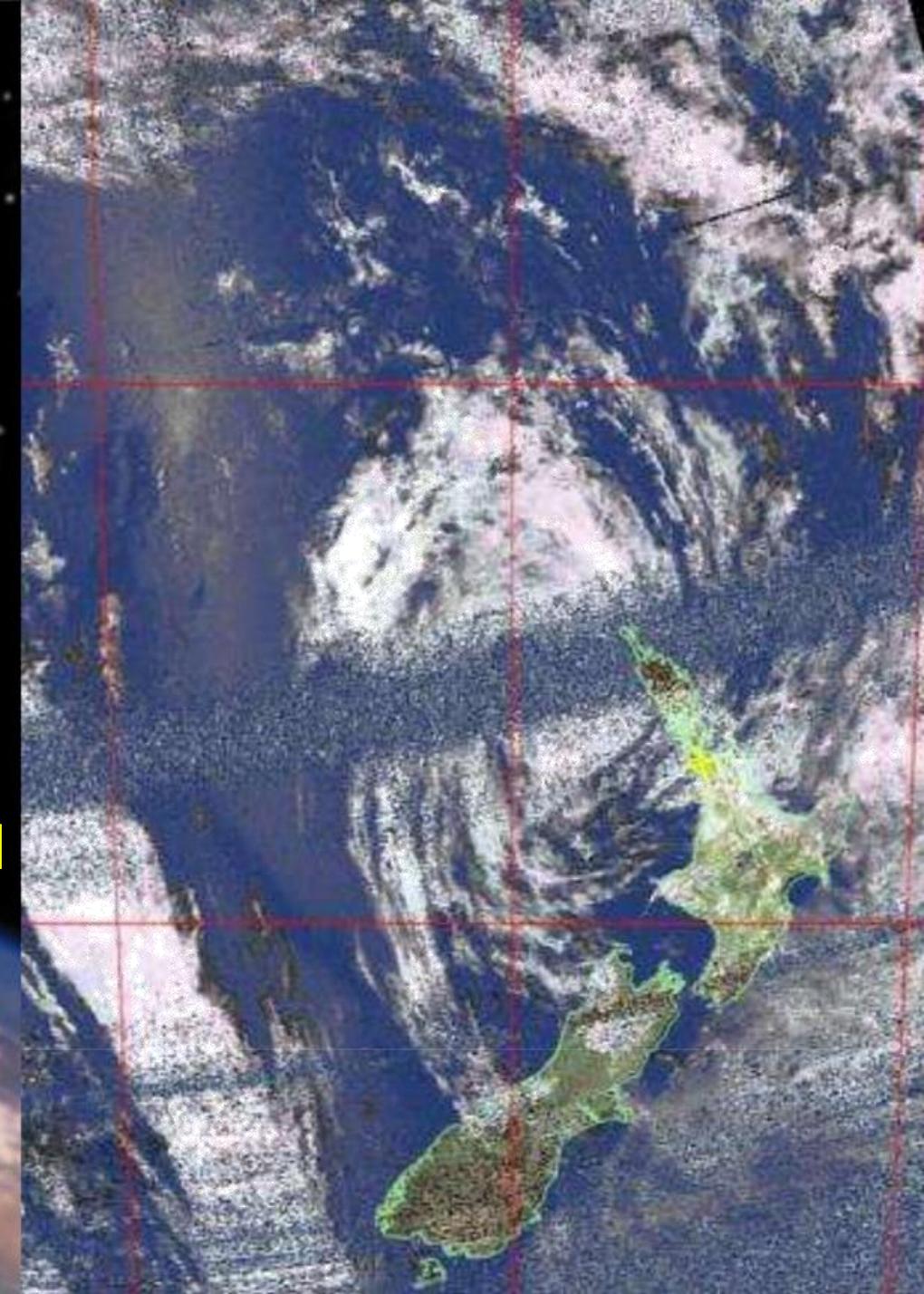
NOAA 15 - 137.6200 MHz

NOAA 18 - 137.9125 MHz

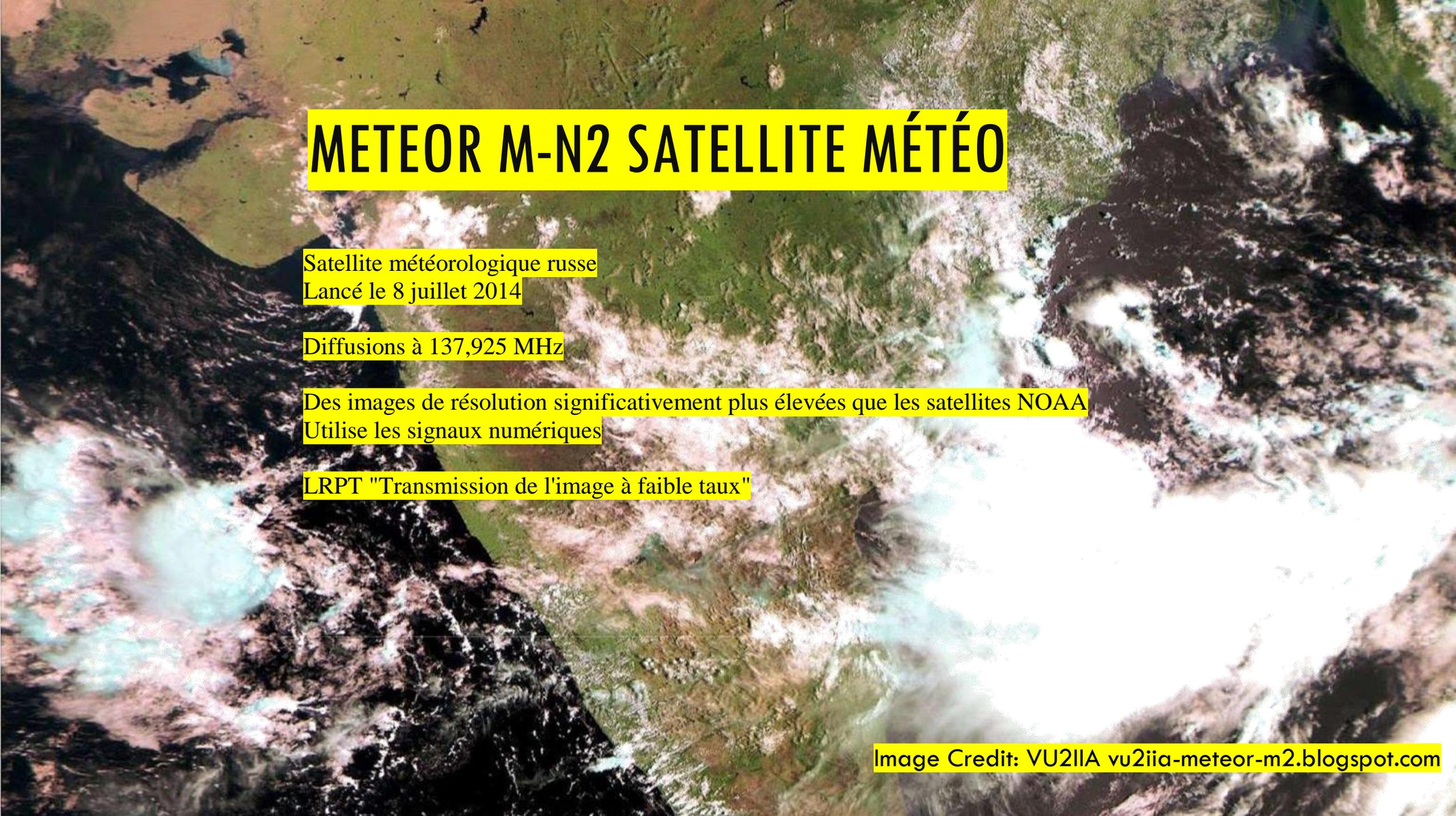
NOAA 19 - 137.1000 MHz

Transmet un signal analogique "APT" (transmission automatique de l'image)

Passeront tous les lieux sur terre plusieurs fois en un jour



METEOR M-N2 SATELLITE MÉTÉO

A satellite image of Earth showing a large area of white and grey clouds over a landmass, likely North America. The surrounding areas are green and brown, representing vegetation and terrain. The image is taken from a high altitude, showing the curvature of the Earth.

Satellite météorologique russe
Lancé le 8 juillet 2014

Diffusions à 137,925 MHz

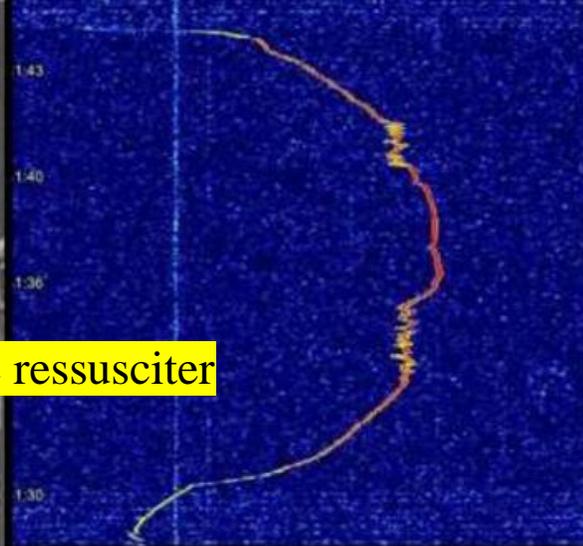
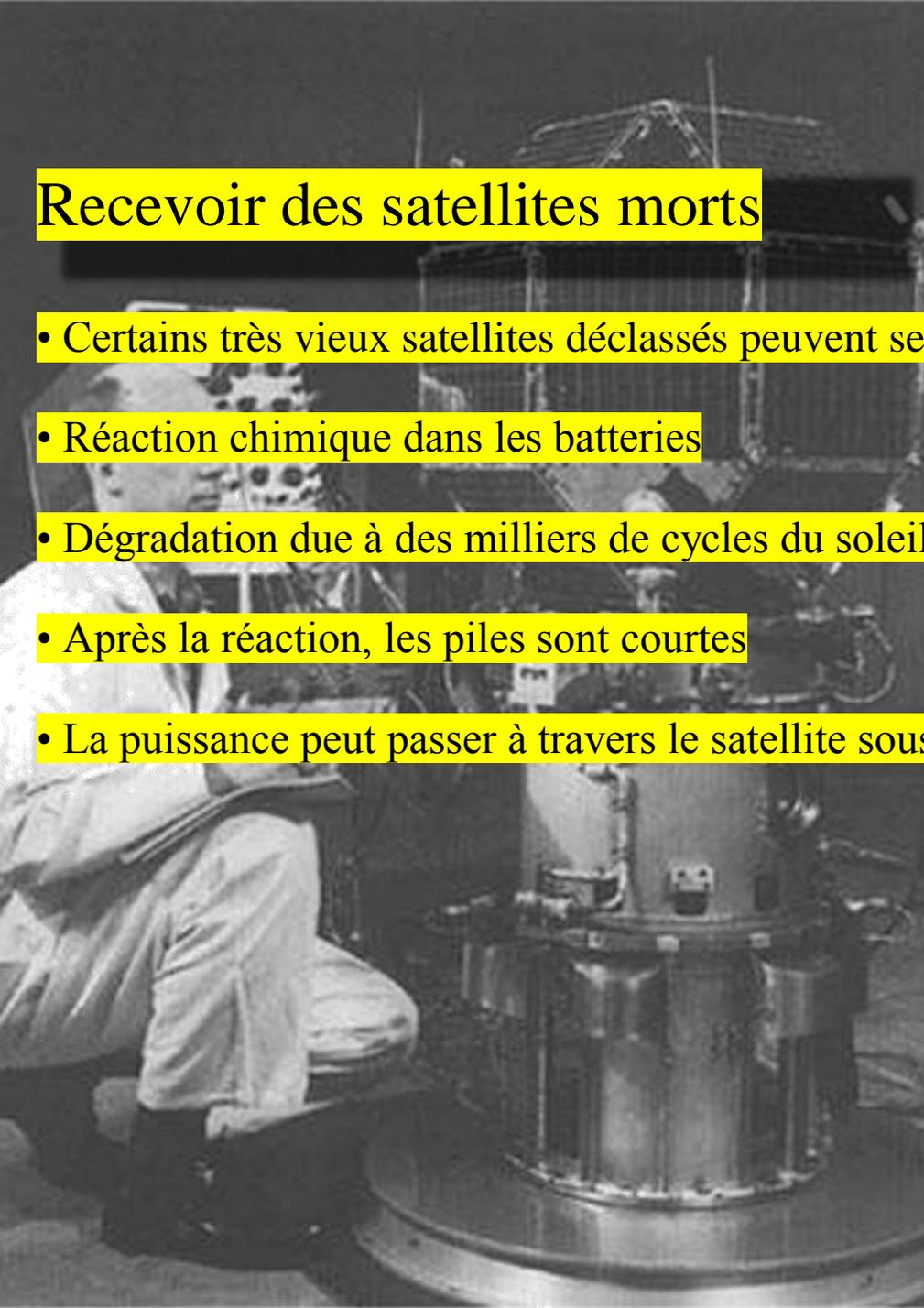
Des images de résolution significativement plus élevées que les satellites NOAA
Utilise les signaux numériques

LRPT "Transmission de l'image à faible taux"

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

Recevoir des satellites morts

- Certains très vieux satellites déclassés peuvent se ressusciter
- Réaction chimique dans les batteries
- Dégradation due à des milliers de cycles du soleil
- Après la réaction, les piles sont courtes
- La puissance peut passer à travers le satellite sous le soleil



NOAA 19

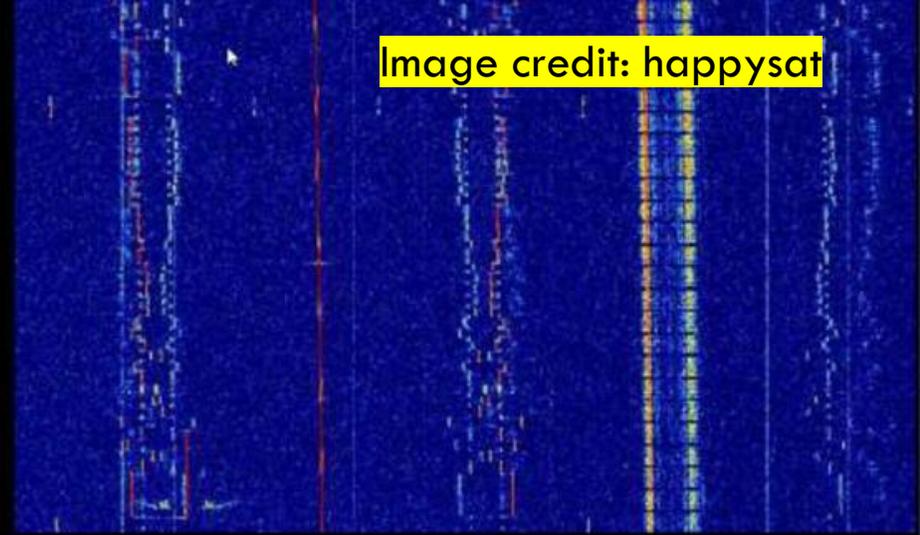
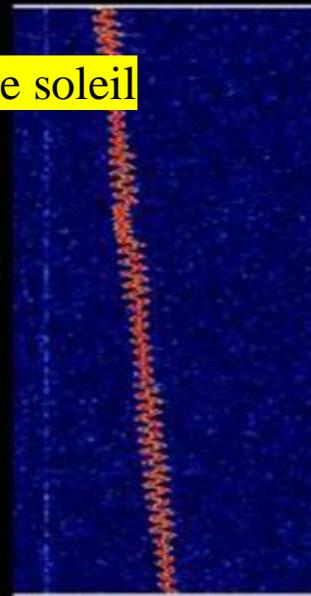
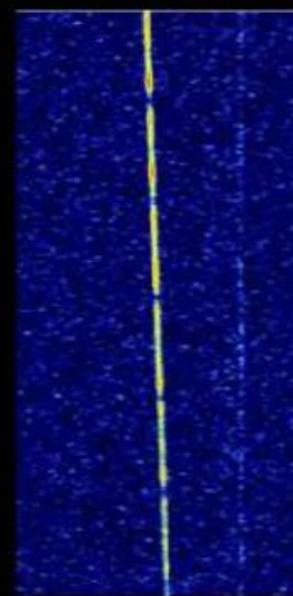


Image credit: happysat

Transit 5B



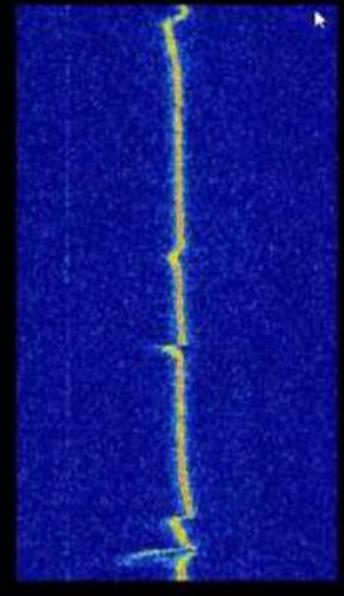
Transit 5B



LES-1



Tiros-1



Aloutte

SATNOGS

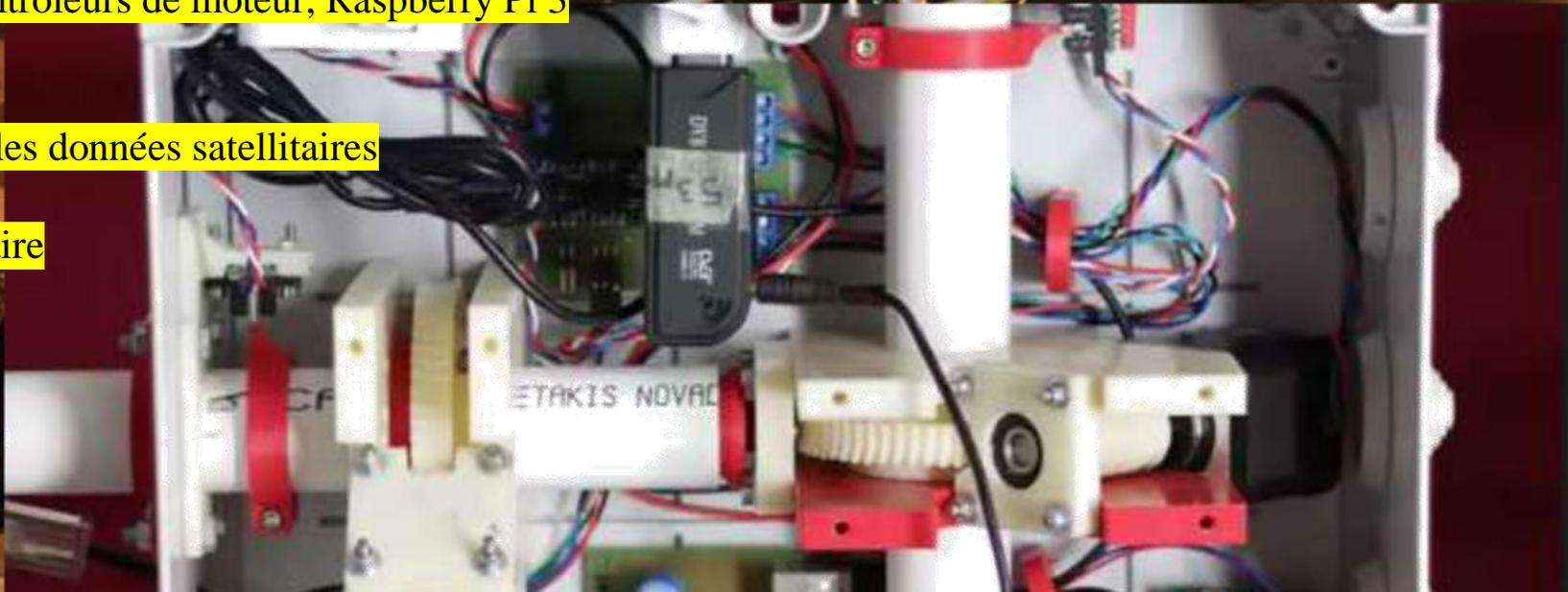
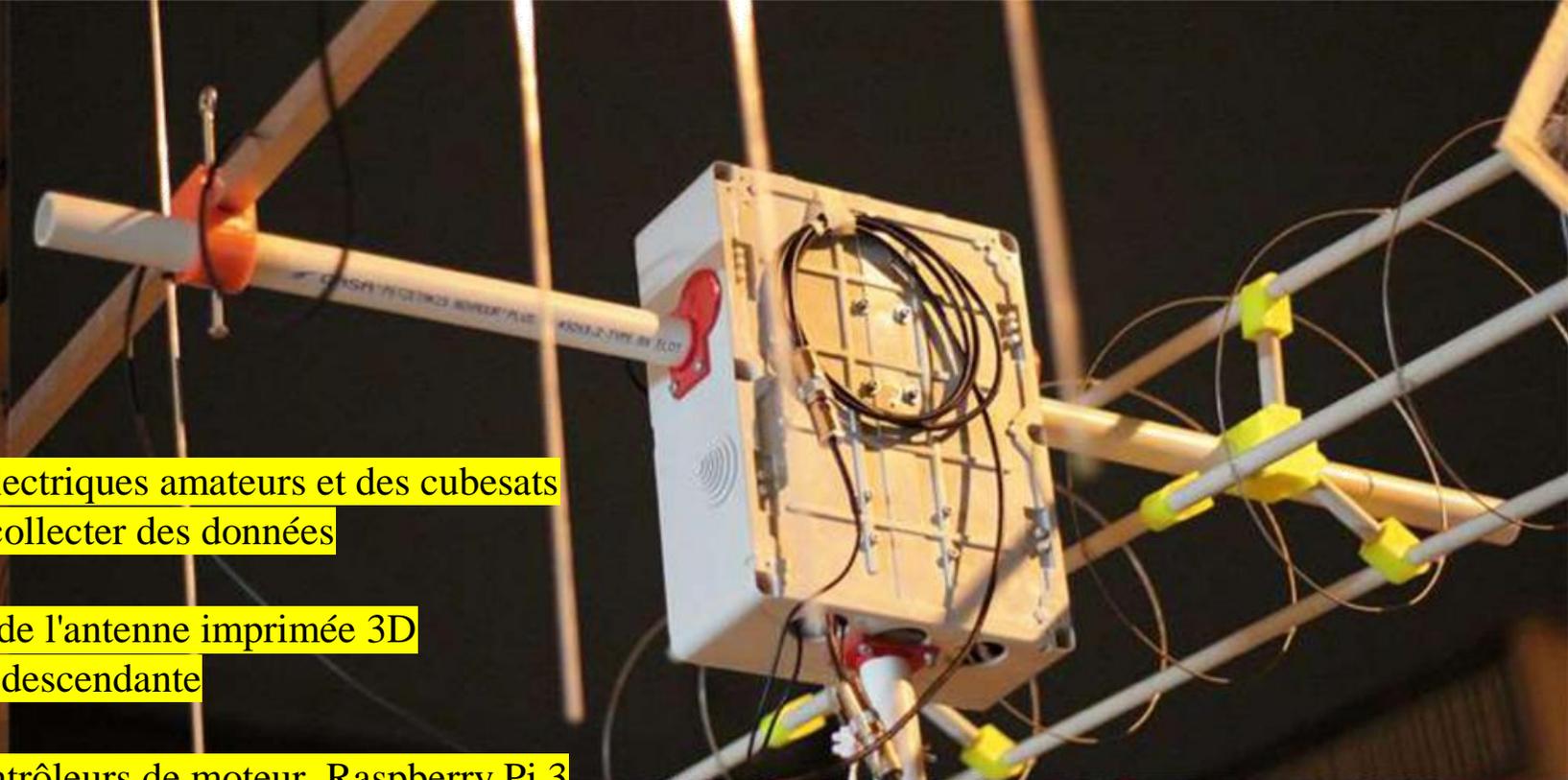
Vaste augmentation des satellites radioélectriques amateurs et des cubesats lancés Pas assez de stations au sol pour collecter des données

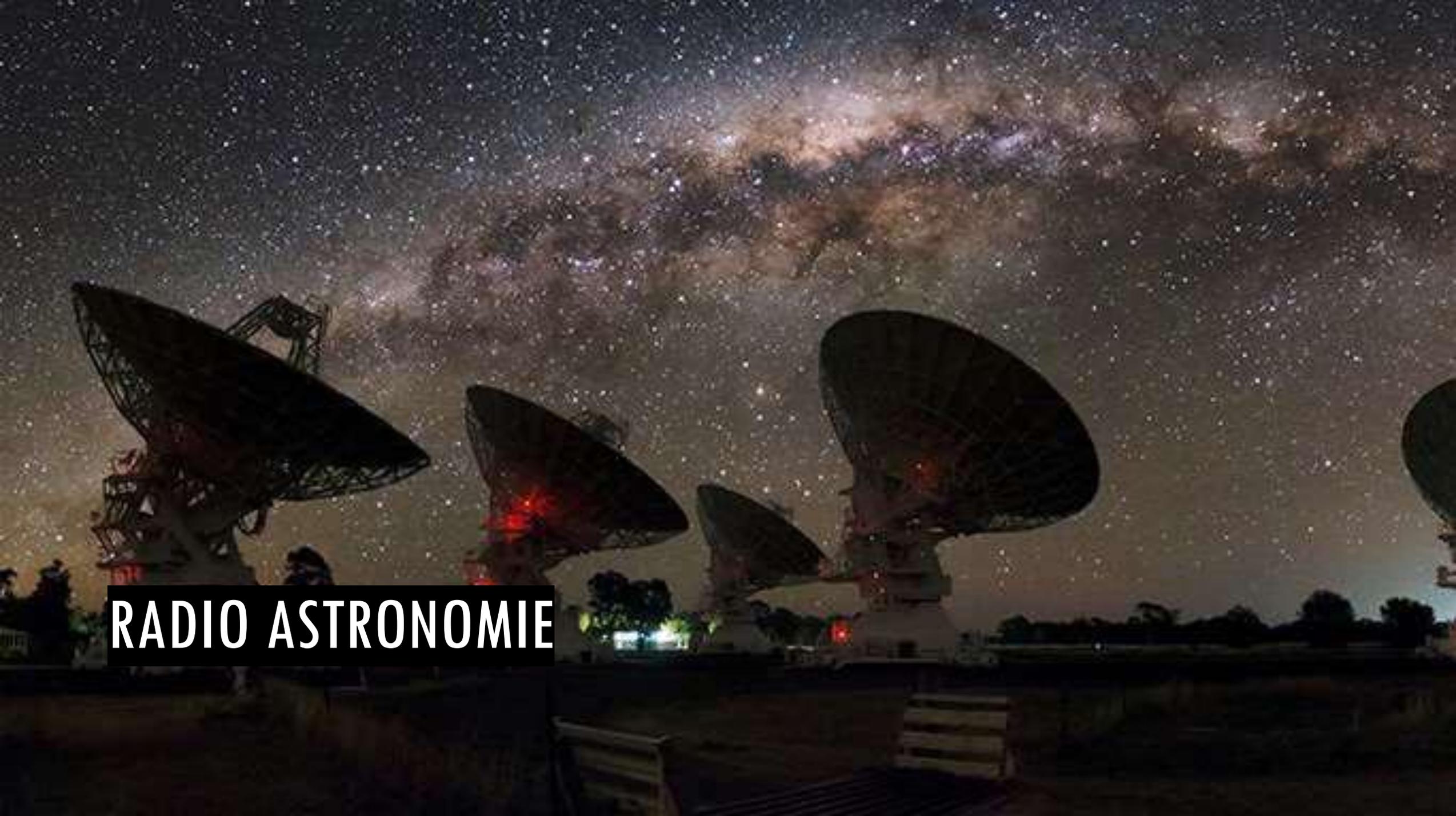
Solution SatNOGS: système de rotation de l'antenne imprimée 3D
Suivi automatique par satellite et liaison descendante

À l'intérieur: RTL-SDR, engrenages, contrôleurs de moteur, Raspberry Pi 3 connectés à internet

Collecte et téléchargement automatique des données satellitaires

ThumbNet / ThumbSat un projet similaire





RADIO ASTRONOMIE

DÉTECTION DE TEMPÉRATURE METEORIELLE

Utilisez le RTL-SDR comme détecteur / compteur de météores

Les météores quittent derrière des sentiers d'air ionisé réfléchissant RF

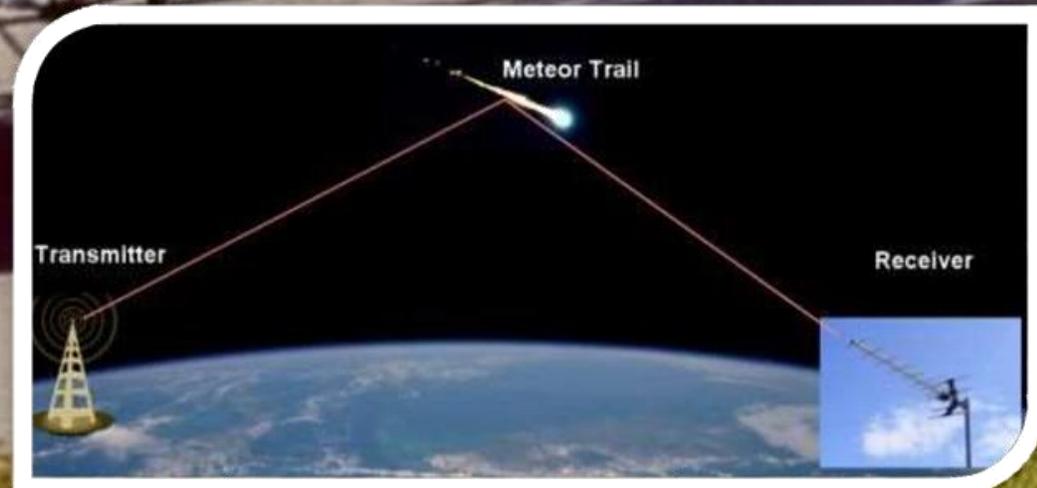
Pointer une antenne directionnelle au ciel

Écoutez les réflexions des émetteurs puissants à des centaines de kilomètres

Les émetteurs que vous pouvez utiliser comprennent
Graves Radar (Europe) ou autre radar

Tours de télévision

livemeteors.com



DÉTECTION D'HYDROGENE ET GALACTIQUE

L'hydrogène est l'élément le plus commun de l'univers

L'hydrogène émet du bruit radio à 21cm (1420.4058 MHz)

Pointez une antenne vers le haut vers le ciel vers beaucoup d'hydrogène et vous pouvez voir la pointe du spectre de fréquence.

Grosse pointe dans notre plan galactique, moins dans l'espace vide.

Équipement nécessaire:

RTL-SDR

Figure de bruit faible LNA + Amplis de ligne

Filtres

Antenne à grand gain, Yagi, corne etc.

DÉTECTION DE PULSARS



- Rotation de l'étoile neutre
- Bruit de bande large sur une large gamme de fréquences
- Le récepteur RTL-SDR enregistre des données de QI brutes
- Algorithmes mathématiques nécessaires pour détecter le pulsar

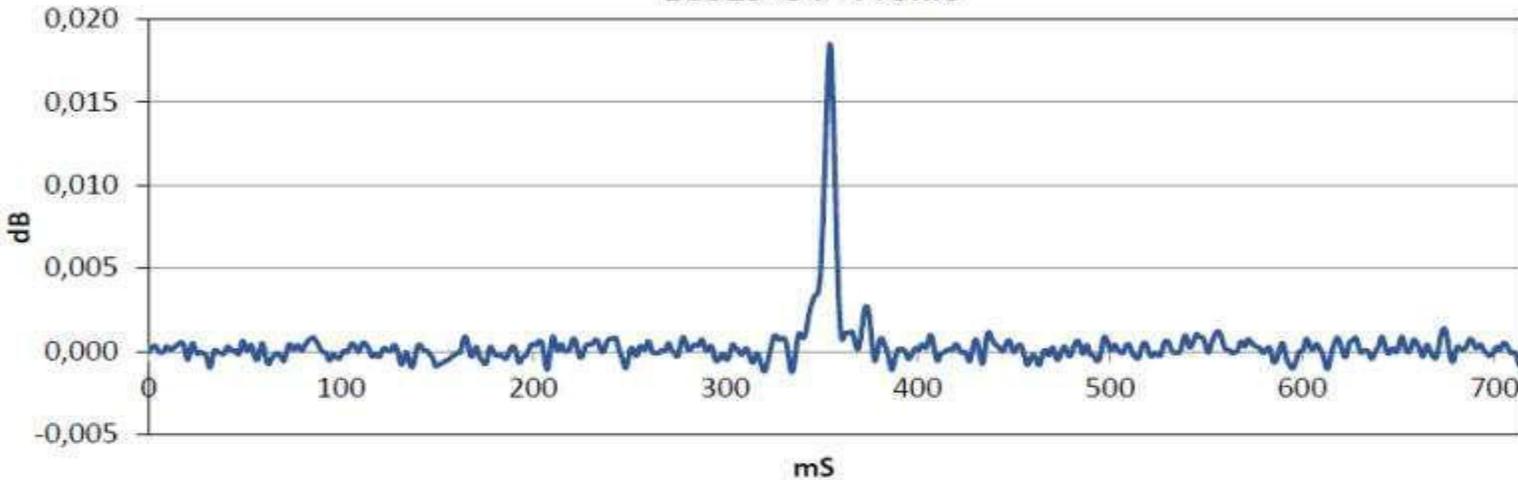


Peter East et Guillermo Gancio (plat 30M à l'Institut Argentín de Radio-Astronomie)



• neutronstar.joataman.net

B0329+54 - Profile



A low-angle, upward-looking photograph of a ship's mast. The mast is a central vertical pole with several horizontal arms extending outwards. At the top of the mast is a large, circular, metallic structure, possibly a radar scanner or a weather instrument. Below this, there are several smaller, cylindrical antennas or sensors mounted on the horizontal arms. The background is a clear, bright blue sky. A yellow banner with black text is overlaid at the bottom of the image.

QRM DETECTION, DIRECTION, RADAR

PASSIVE RADAR

Semblable à la détection des météorites
Utilise les reflets d'un puissant émetteur de diffusion

Mais si vous utilisez deux antennes
Vous pouvez obtenir une vue radar 2D

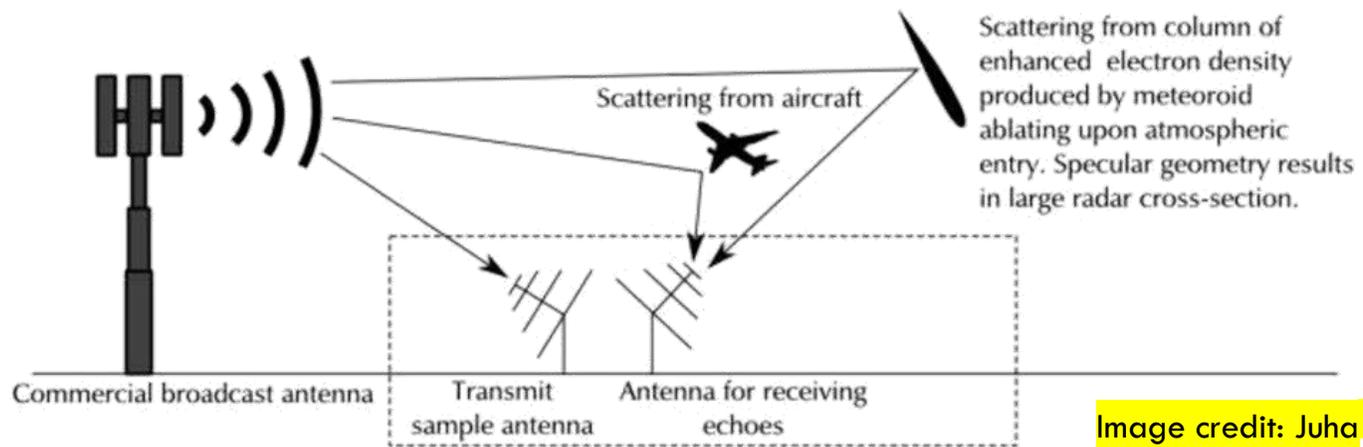
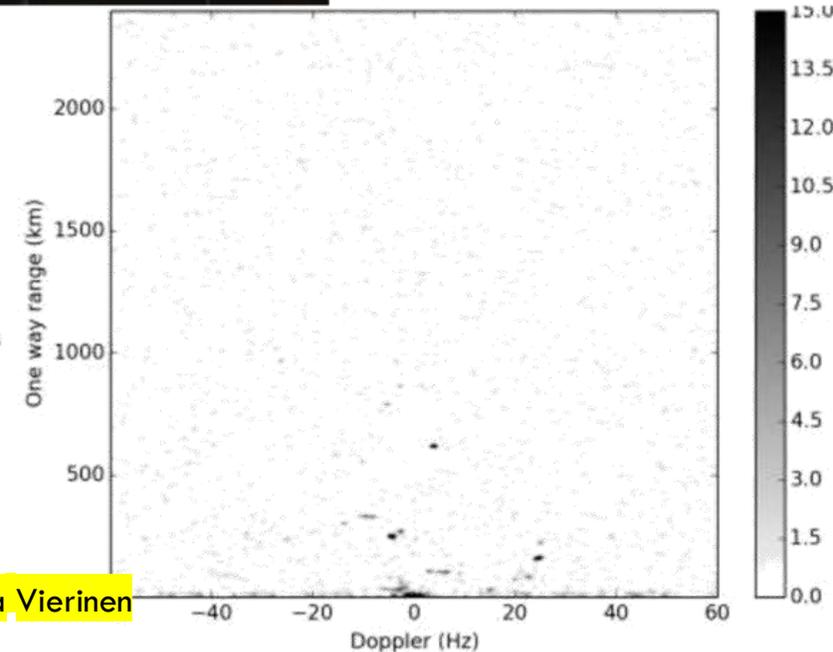


Image credit: Juha Vierinen



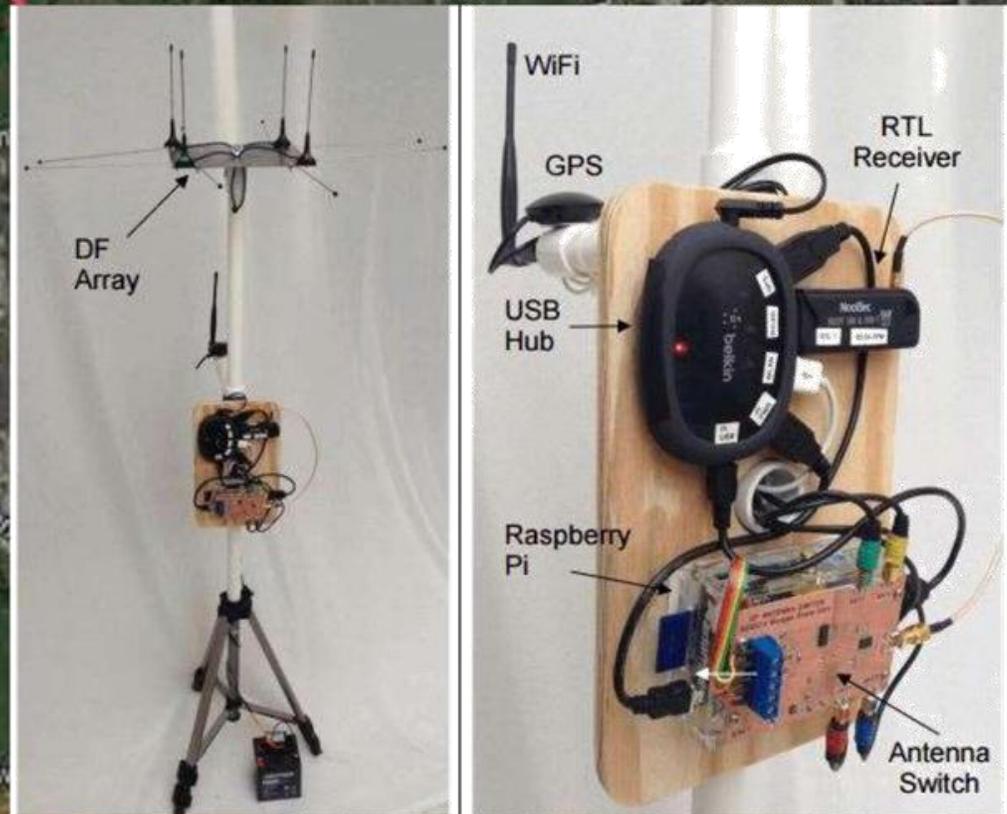
Nodes:
3

SIGNAL DIRECTION FINDING

Système RasHAWK

Basé sur les produits Raspberry Pi et REDHAWK DSP

Utilise la commutation d'antenne Détermine le palier du signal
Combinez plusieurs unités pour identifier l'émetteur

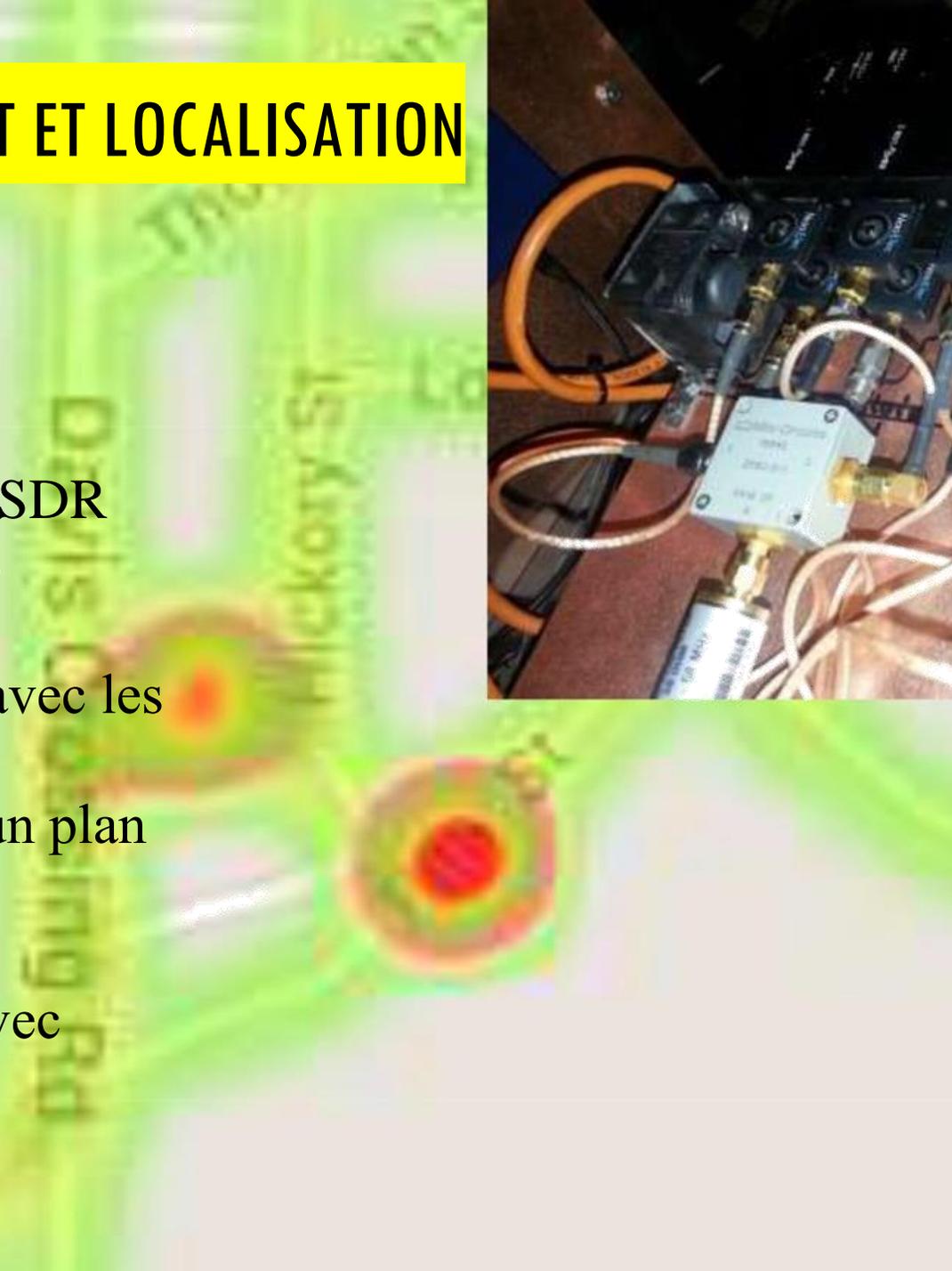


QRM/ DÉTECTION DU BRUIT ET LOCALISATION

- Tim Havens "Driveby"
Système:QRM

Détecteur

- Utilise plusieurs dongles RTL-SDR fonctionnant sur un Odroid XU3
- Analyse plusieurs bandes
- Enregistrez les niveaux QRM avec les données GPS
- Trouver les points chauds sur un plan thermique
- Source trouvée: Pôles moteur avec connexion au sol cassé



SATELLITES L-BAND



RECEVOIR L'OUTERNET

Un moyen (téléchargement uniquement) service de filtrage par satellite
Utilise les satellites Inmarsat / Alphasat sur la bande L

Quelles données pouvez-vous recevoir?
Dernières nouvelles

Mise à jour Météo

Répétiteurs de répétition de radio amateur (ISS APRS, AMSAT etc)

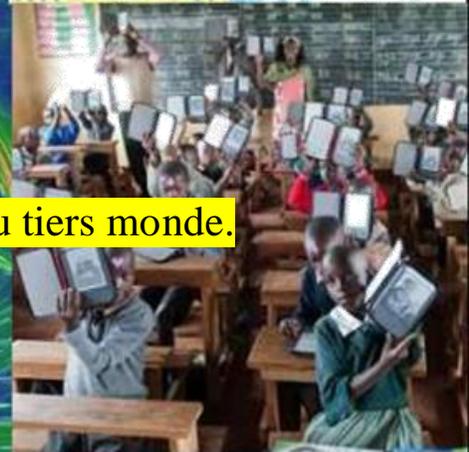
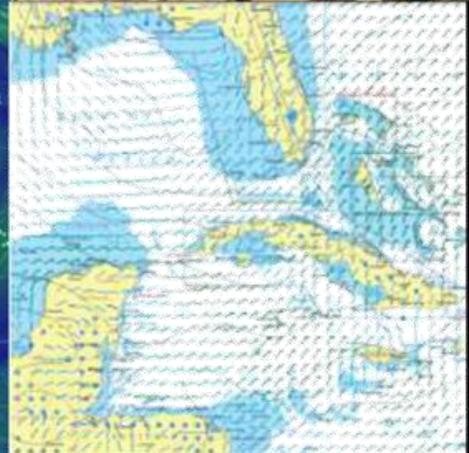
Articles de Wikipedia

Fichiers Grib (pour les marins en mer)

Livres gratuits

Bon pour les pêcheurs de catastrophe, les marins, les régions éloignées, les pays avec Internet censuré, les pays du tiers monde.

Outernet utilise des récepteurs RTL-SDR basés



QU'EST-CE QUE VOUS AVEZ BESOIN POUR RECEVOIR OUTERNET

Dongle RTL-SDR v3 ou E4000 (avec t de polarisation)

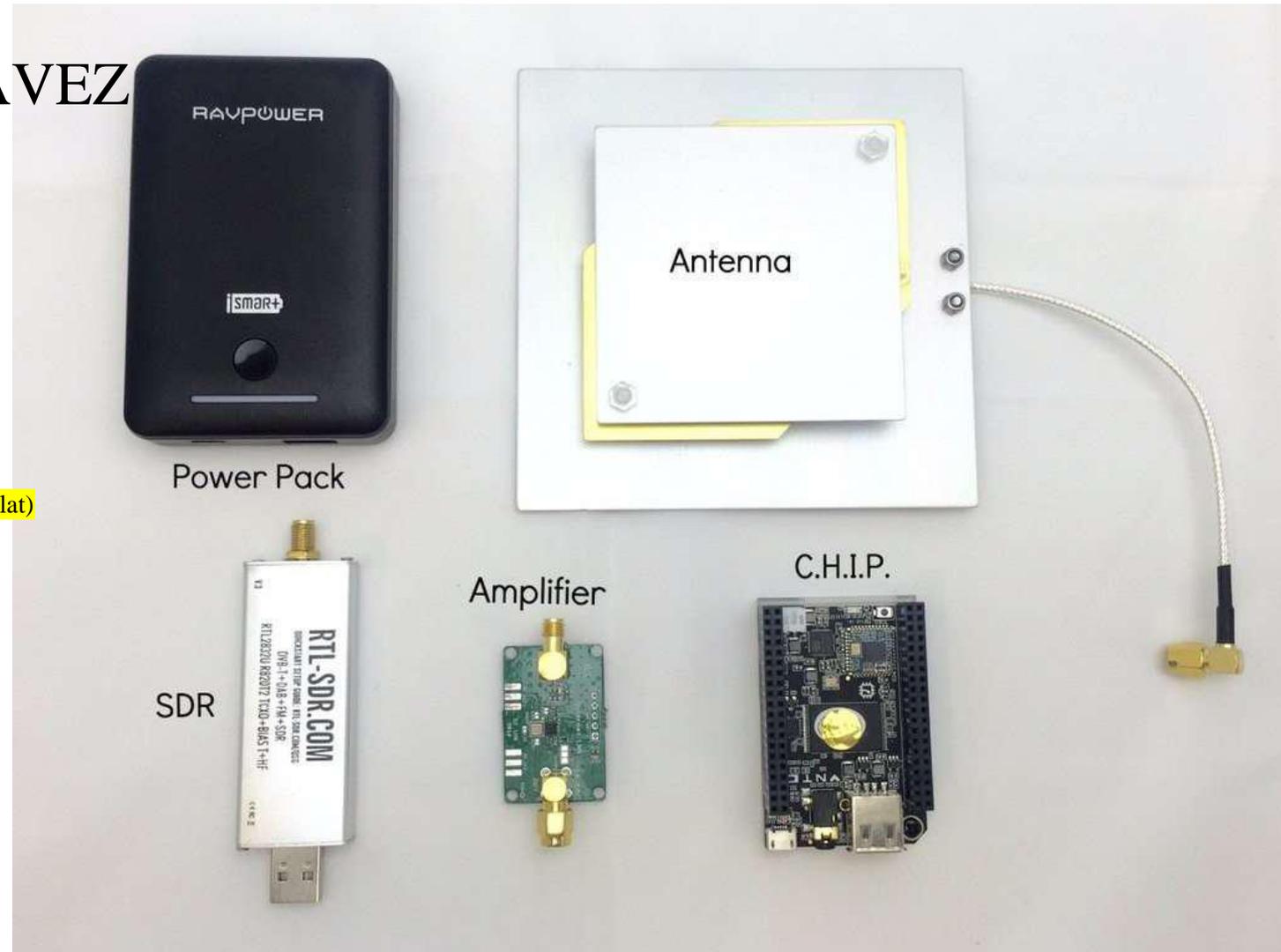
Un LNA (avec filtre)

Antenne satellite à 1,5 GHz en bande L (comme un patch ou un plat)

Ordinateur C.H.I.P

Outernet travaille sur une solution entièrement intégrée

www.outernet.is



SATELLITES DE L-BANDE: SÉCURITÉ INMARSAT

Inmarsat STD-C "SafetyNET" émission de messages de sécurité

Principalement la météo, la recherche et le sauvetage, les rapports d'incidents, les déploiements de câbles sous-marins, les exercices militaires et les avertissements de pirates pour les marins.

CINQ ROBBERS ARMÉS AVEC DES COUTEAUX LONGS DANS UN BATEAU À GRAU VITESSE PETIT DÉLIVRÉ APPROUVE UN TRANSPORTE À BULLEUX EN COURS. L'UN DES ROBBERS ATTENTE DE PLACER LE NAVIRE À L'AIDE D'UN CROCHET ATTACHÉ À UNE CORDE. ALERT CREW AVISÉ LE ROBBER ET ÉLEVÉ L'ALARME ET L'ÉQUIPE RUSHED À L'EMPLACEMENT. AUCUNE HEURE DE L'ALARME ET VÉRIFIE L'ALERTE DE L'ÉQUIPE, LES ROBBERS ONT ABORDÉ L'ATTAQUE ATTENDU ET DÉPLACÉE.

INGÉNIEUR DE DONNÉES A BORD D'UN PRODUIT DE TRANSFERT DE TANKER DÉCOUVERTE DE TROIS ROBBERS DANS LA CHAMBRE DE MOTEUR PRÈS DE L'ESPACE INCINÉRATEUR. LES ROBBERS RAN À LEUR BATEAU. UNE RECHERCHE A ETE EFFECTUÉE. NON ROBBERS TROUVÉ À BORD ET RIEN A ÉTÉ ROUILLÉ.

Softwares
www.inmarsatdecoder.com

Tekamanoid <http://www.tekmanoid.com/egc.shtml>

SATELLITES L-BAND: IRIDIUM

Iridium est un service mondial par satellite avec plus de 72 satellites

Fournit des services tels que

Les téléavertisseurs mondiaux,

Les téléphones satellites,

Le suivi et la gestion de la flotte,

divers services pour les urgences,

les avions, les navires et les secrets militaires.

Les chercheurs en sécurité Stefan "Sec" Zehl et Schneider a décodé Iridium

Peut recevoir des appels et des messages de téléavertisseur

Dans leur conférence, ils démontrent l'interception d'un appel du 310e avion militaire du C-37 de l'escadron aérien.

Facile, mais pas trop facile à écouter.



L-bandes SATELLITES: EXEMPLE DE CE QUE STEFAN ET SCHNEIDER REÇU

"Heli sur la route. Aussi, les batteries dont vous avez besoin?"

Joe, passez au tacsat pour moi dès que possible, votre grille est erronée, devrait être 40 xxxx 89681 21960. Vous allez 8 km au mauvais sens.

nos arcs ne sont pas sur la cible.

La grille que j'ai de vous est xxxx 4882 et l'emplacement de l'ennemi xxxx 4804.

J2 indique le compromis Op. Extraire immédiatement. Agissez par HF. "

"Appel socrates pour les mises à jour d'information, nous avons une cible de qualité. Après l'Allemagne, appelez le socrate sur la communication bleue et préparez-vous au travail. Il y a un scorpion rouge à la voile.

Vous devez appeler xxxx ou xxxx. Nous sommes ce que c'est mieux si vous appelez à partir de xxxx ou xxxx.

Dites au barman qu'ils doivent nous parler avant de pouvoir effectuer le paiement.

En tout cas, vous devez passer l'Allemagne pour le faire écouter White, ouvrir long homme! Rapport avant ou au Venezuela "



The image features a central glowing padlock icon, rendered in a light blue and white color scheme, set against a dark blue background filled with intricate, glowing white and light blue circuit traces. The traces radiate outwards from the padlock, creating a sense of digital connectivity and security. The overall aesthetic is futuristic and technological.

SÉCURITÉ RF

RÉPARTIR L'ENTROPIE À PARTIR DE BRUIT ATMOSPHERIQUE

Un ordinateur ne peut pas générer de vrais nombres aléatoires seulement pseudo-aléatoires

Un véritable hasard peut être obtenu à partir de mouvements de souris et de clavier
Mais qu'en est-il des ordinateurs embarqués (par exemple, routeurs, périphériques IoT) sans entrées?

Un hasard réel est nécessaire pour la cryptographie et les systèmes de sécurisation.
Si les touches ne sont pas vraiment aléatoires, elles peuvent être devinées / calculées.

Un programme RTL-SDR appelé rtl_entropy peut être utilisé pour rassembler des nombres aléatoires vrais

Rassembler le bruit atmosphérique (statique). Rayonnement galactique, éclair.

RTL-SDR / USB Configure VFO 0.024.641.000

AM LSB USB
DSB CW RAW
0
Blackman-Harris
Filter width 9610 Filter order 10
CW Shift 89 500
Step size 500 Hz
grid
Swap I & Q
Mark Peaks

RF LEAKY HP LAPTOP: SECURITY FLAW

Le spectre de fréquence de navigation cronek utilisateur Reddit avec son ordinateur portable Trouve un signal impair à 24 MHz

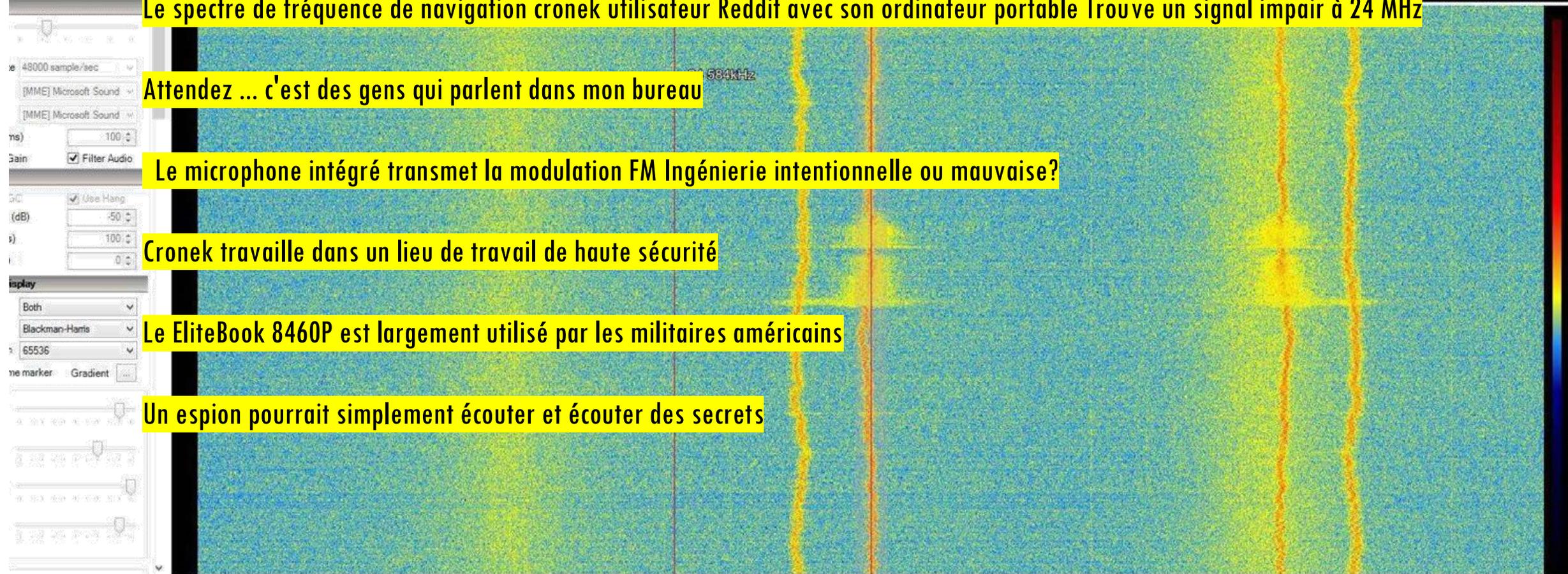
Attendez ... c'est des gens qui parlent dans mon bureau

Le microphone intégré transmet la modulation FM Ingénierie intentionnelle ou mauvaise?

Cronek travaille dans un lieu de travail de haute sécurité

Le EliteBook 8460P est largement utilisé par les militaires américains

Un espion pourrait simplement écouter et écouter des secrets



Zoom
Contrast
Speed

ANALYSE ET DÉCODAGE GSM

Filter: **gsm** Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
511	4056.82466700	127.0.0.1	127.0.0.1	GSM TAP	81	(CCCH) (SS)
512	4056.83141000	127.0.0.1	127.0.0.1	GSM TAP	81	(CCCH) (SS)
513	4056.835					
514	4056.841					
515	4056.844					
516	4056.85004000	127.0.0.1	127.0.0.1	GSM TAP	81	(CCCH) (RR) Paging Request Type 1
517	4056.85449700	127.0.0.1	127.0.0.1	GSM TAP	81	(CCCH) (RR) Paging Request Type 1
518	4056.86118200	127.0.0.1	127.0.0.1	GSM TAP	81	(CCCH) (RR) Paging Request Type 1
519	4056.864					
520	4056.871					
521	4056.874					
522	4056.88082900	127.0.0.1	127.0.0.1	GSM TAP	81	(CCCH) (SS)
523	4056.88507000	127.0.0.1	127.0.0.1	GSM TAP	81	(CCCH) (SS)
524	4056.89035100	127.0.0.1	127.0.0.1	GSM TAP	81	(CCCH) (RR) Paging Request Type 1

La sécurité du téléphone portable GSM (2G) est cassée

Utilisez un RTL-SDR pour recevoir des textes et des appels téléphoniques

Ne vous inquiétez pas - il est encore assez difficile

Facile à faire pour votre propre téléphone

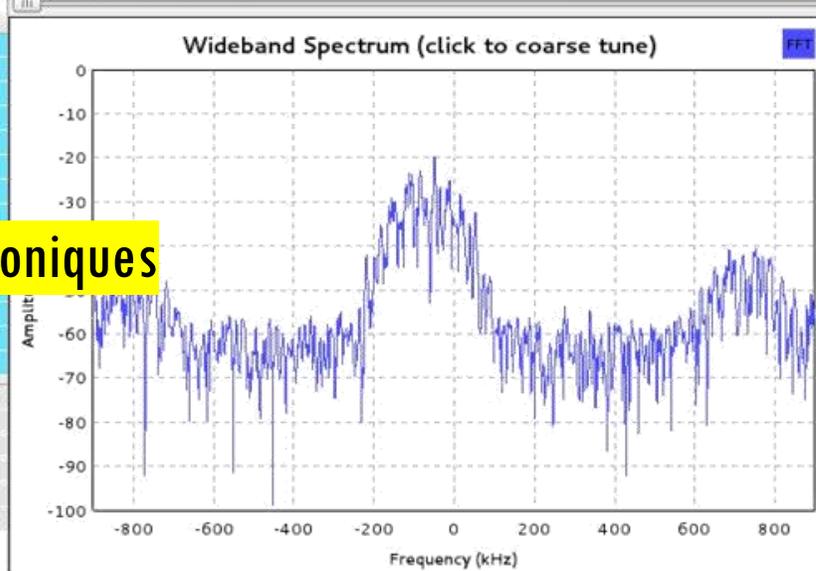
Très difficile à faire pour les autres téléphones

besoin d'un ordinateur rapide et beaucoup de temps de décryptage

```

Frame 520: 81 bytes on wire (capture length 81) captured on interface eth0
  Ethernet II, Src: vmxnet3 (08:00:00:00:00:00), Dst: 127.0.0.1
  Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
  User Datagram Protocol, Src Port: 49162 (49162), Dst Port: gsmmap (4729)
  GSM TAP Header, ARFCN: 0 (Downlink), TS: 0, Channel: BCCH (0)
  GSM CCCH - Syst
    L2 Pseudo Length: 81
    Protocol Discriminator: 0
    Message Type: System information type 3
    Cell Identity - CI (35426)
    Location Area Identification (LAI)
      Location Area Code (LAC) (0000)
      Mobile Country Code (MCC) (00)
      Mobile Network Code (MNC) (00)
    Control Channel (CC)
    Cell Options
    Cell Selection
    RACH Control
    SI 3 Rest Octets
  
```

Center Frequency: 936.6M Automatic Gain RF Gain: 0



Trace Options

- Peak Hold
- Average
- Avg Alpha: 0.3000
- Persistence
- Persist Alpha: 0.2600
- Trace A Store
- Trace B Store

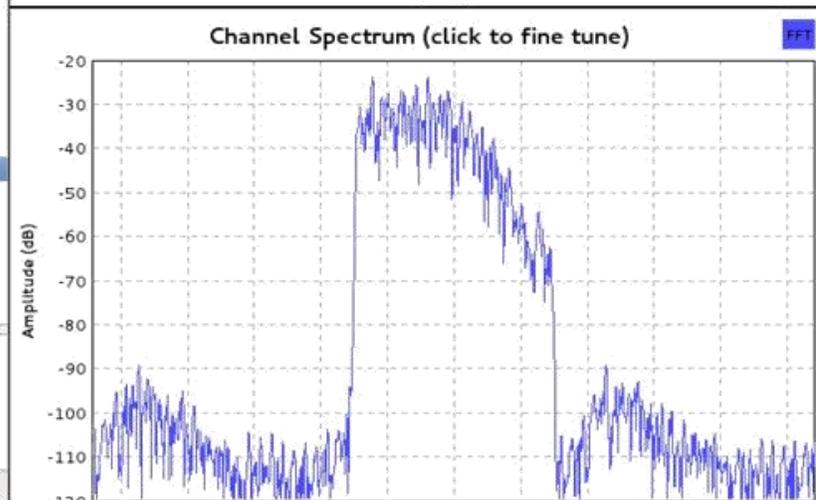
Axis Options

dB/Div: +

Ref Level: +

Autoscale

Stop



Trace Options

- Peak Hold
- Average
- Avg Alpha: 0.3000
- Persistence
- Persist Alpha: 0.2600
- Trace A Store
- Trace B Store

Axis Options

dB/Div: +

Ref Level: +

Autoscale

POUR UTILISER UN RTL-SDR

Dejan Ornič

Étudiant de 26 ans à la "Faculté de justice et de justice pénale de l'Université de Maribor" en Slovénie

Projet de recherche pour enquêter sur les vulnérabilités de TETRA

TETRA - communications numériques souvent utilisées par la police / EMS en Europe.

En utilisant son RTL-SDR, il a trouvé une mauvaise configuration dans la mise en œuvre slovène de TETRA: la sécurité était brisée

Police notifiée

Aucune réponse ou action prise pendant 2 ans

Alors il a ramené son histoire à l'agence de presse locale

La police accède à sa maison, saisit son ordinateur et RTL-SDR

Compte tenu d'une peine de prison suspendue de 15 mois

PRODUITS SANS FIL D'INGÉNIERIE REVERSE

- Sonnettes
- Capteurs de température et météo
- voitures RC
- Ventilateur de plafond

- Colliers chocs pour chien
- prises de courant alternatif à commande sans fil
- Serrures de porte sans fil
- Capteurs et alarmes domotiques
- Appareils IoT
- feux de signalisation portables
- Affichage du trafic public
- Portes de voiture



Image credit: Bastian Bloessl

MOTORISATEUR D'AUTO-INGÉNIERIE REVERSE

La télémétrie de bus utilisée dans les villes modernes pour les panneaux aux arrêts de bus.

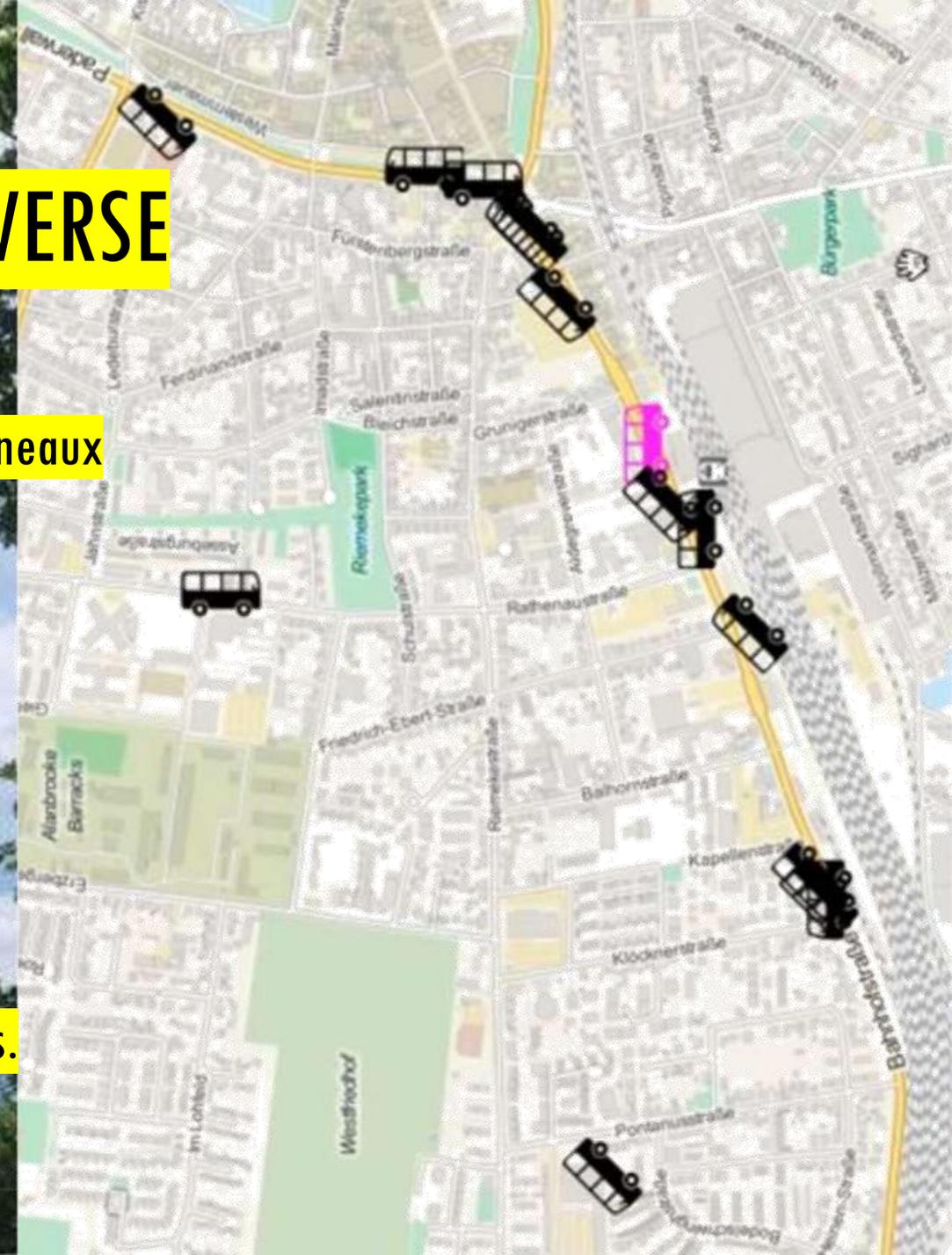
Les données sont transmises sans fil et sont en direct

Bastian Bloessl - Paderborn, Allemagne

Trouvé un signal de télémétrie à 150 MHz

D'autres méthodes de télémétrie comme les sous-porteuses utilisées dans la radiodiffusion FM sont utilisées dans d'autres pays.

Voir le travail d'Oona Raissan à Helsinki, en Finlande.



AUTRES APPLICATIONS

GPS SUR UN ROCKET ÉLEVÉ

La plupart des appareils GPS sont conçus pour échouer si ils voyagent trop vite ou trop haut
COCOM Limit - 1.200 mpg et 59,000 ft.

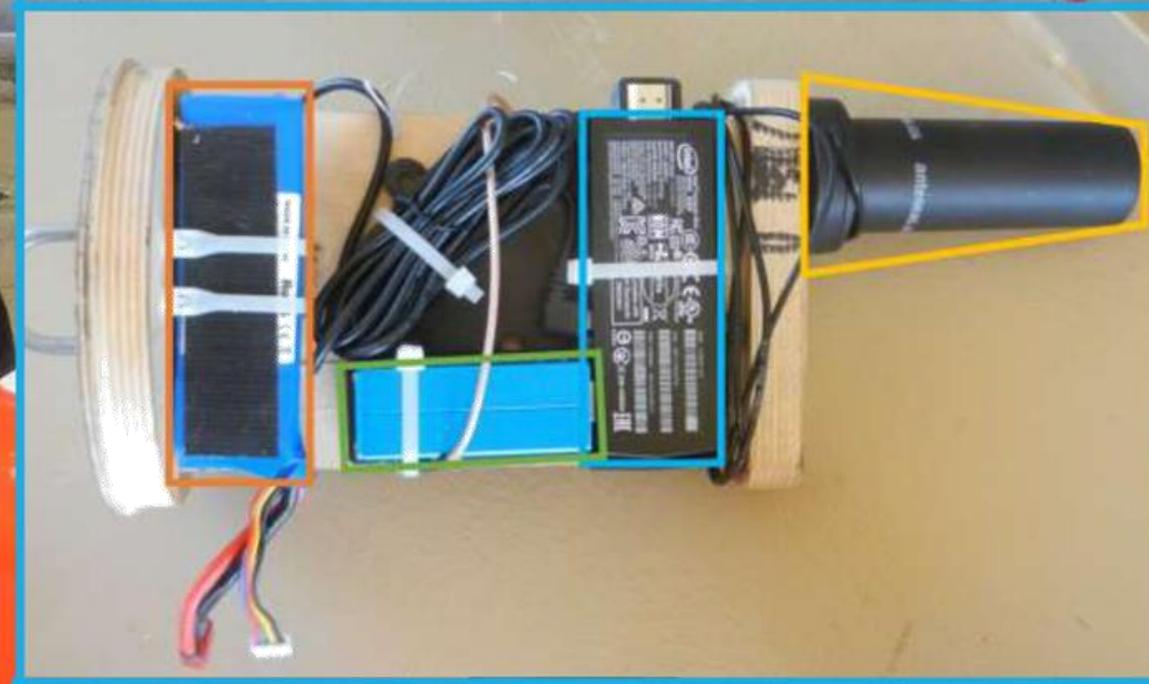
Limite imposée par l'armée américaine

Limite appliquée par les fabricants de matériel GPS.

Philip Hahn & Paul Breed construisent des petites roquettes à haute puissance

La fusée pourrait être trop rapide et trop élevée

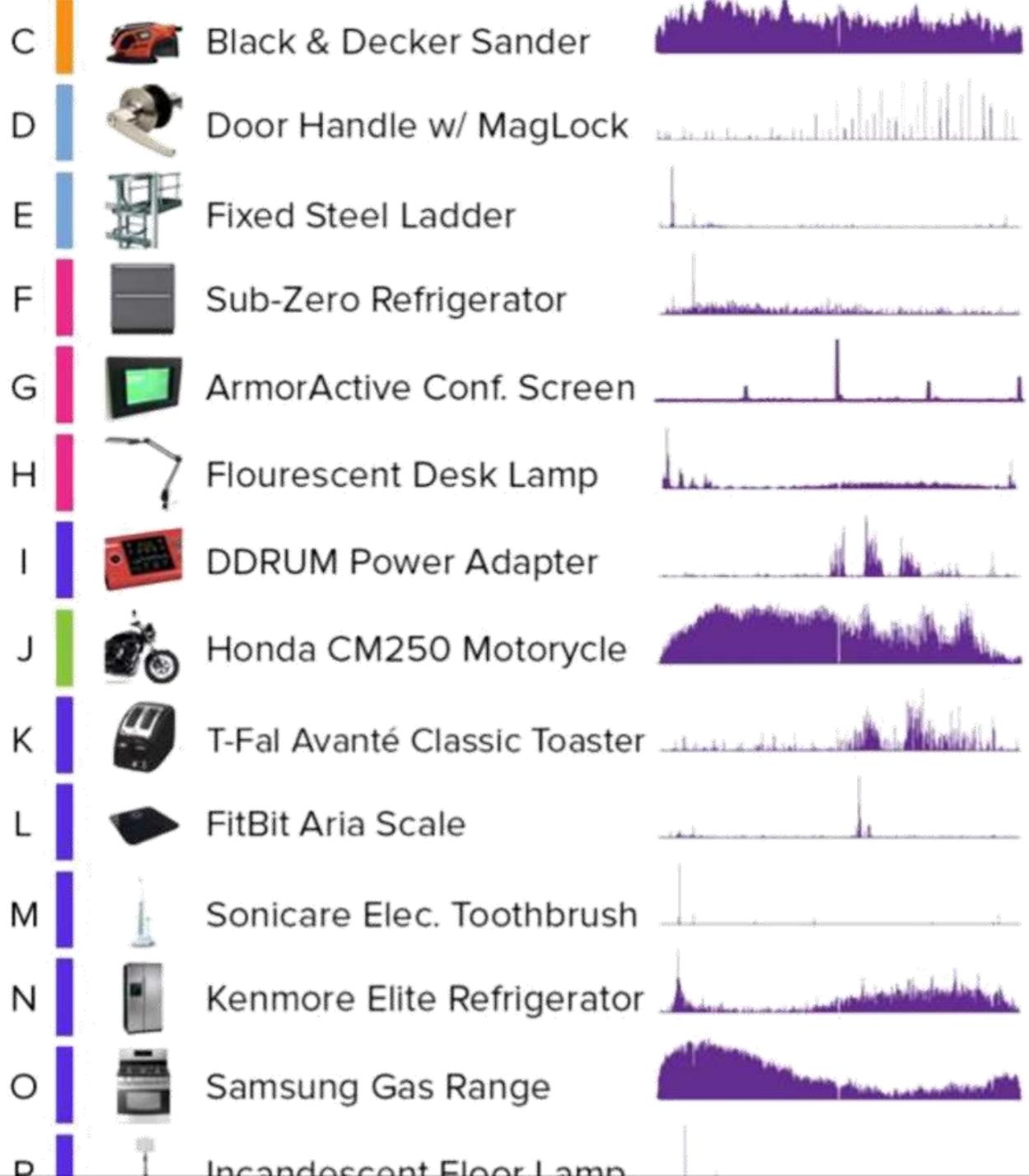
Utilisation d'un logiciel open-source RTL-SDR et GNSS-SDR pour obtenir des corrections de position.



DISNEY'S EM SENSE

Une montre qui sait exactement ce que le porteur touche

Fonctionne en classant EMI RTL-SDR Based



QU'EST-CE QUE J'AI MISSÉ? BEAUCOUP.

Écouter l'ISS

Playstation 3 Reverse Engineering via EMI

Ingénierie inverse d'un défibrillateur cardiaque

Décodage VOR

ACARS

Pagers

Défaite des alarmes IoT et des portes de voiture

Surveillance à distance

Analyse du trafic sans fil

Recherche paranormale de voix électronique

Satellites météorologiques GOES

Bruits de bruit de Jupiter

Détection de décharge partielle

Indicateur de bruit

Recevoir des ballons météorologiques

Utilisation du RTL-SDR en tant que compteur VSWR

Utilisation du RTL-SDR pour tester les filtres RF

Décodage DAB & DRM

Pirates de Milsatcom

CONCLUSION

J'espère que cette conversation vous a inspiré à essayer quelque chose de nouveau avec la radio

Suivez et parcourez l'histoire du blog RTL-SDR.com pour des projets plus intéressants comme celui-ci.

Merci à TAPR de m'avoir invité à faire ce discours

Où puis-je acheter des Dongles RTL-SDR V3 à 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

Données SUPPLÉMENTAIRES

ÉCOUTE DE L'ISS

SSTV Images

Les astronautes parlent pendant les promenades spatiales

Activités de radio amateur

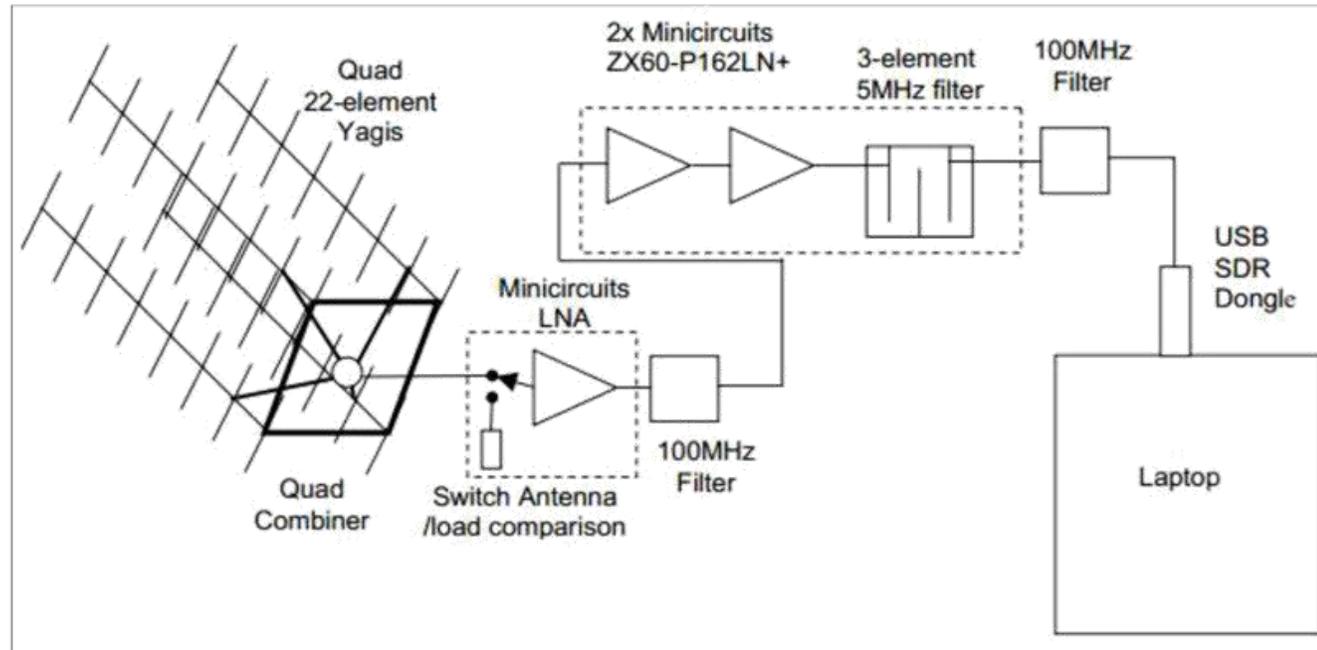
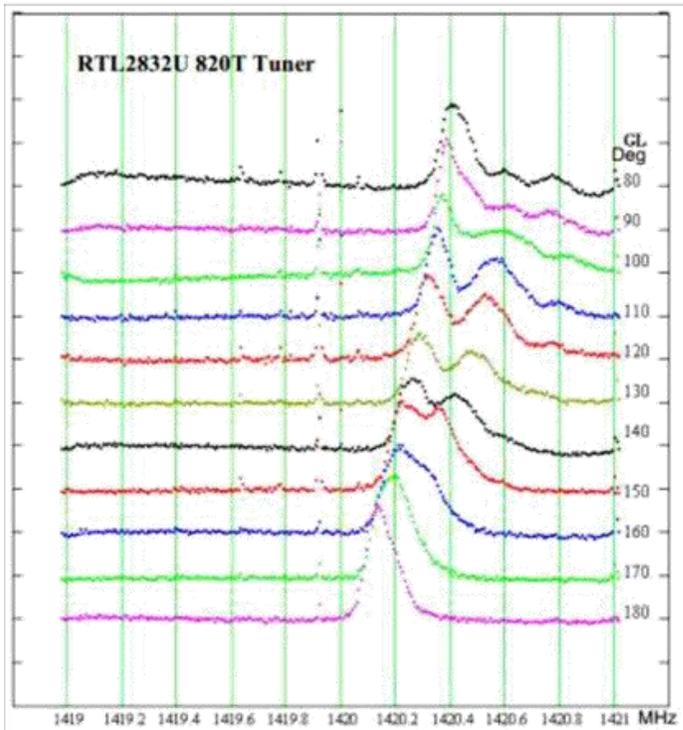
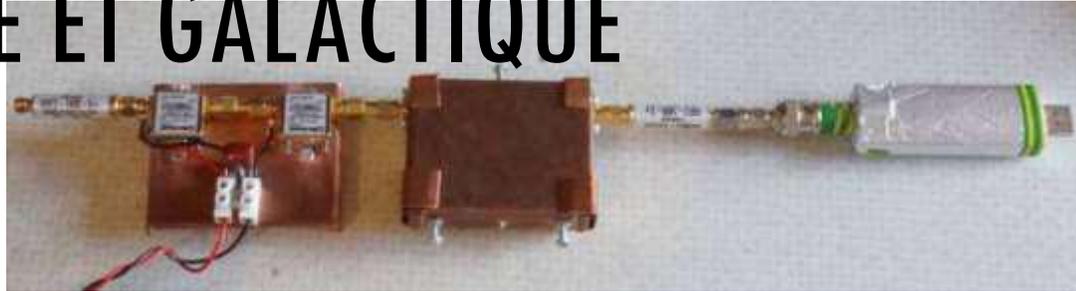
TV numérique amateur



DÉTECTION D'HYDROGENE ET GALACTIQUE

Peter W East

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



QRM/ DÉTECTION DU BRUIT ET LOCALISATION

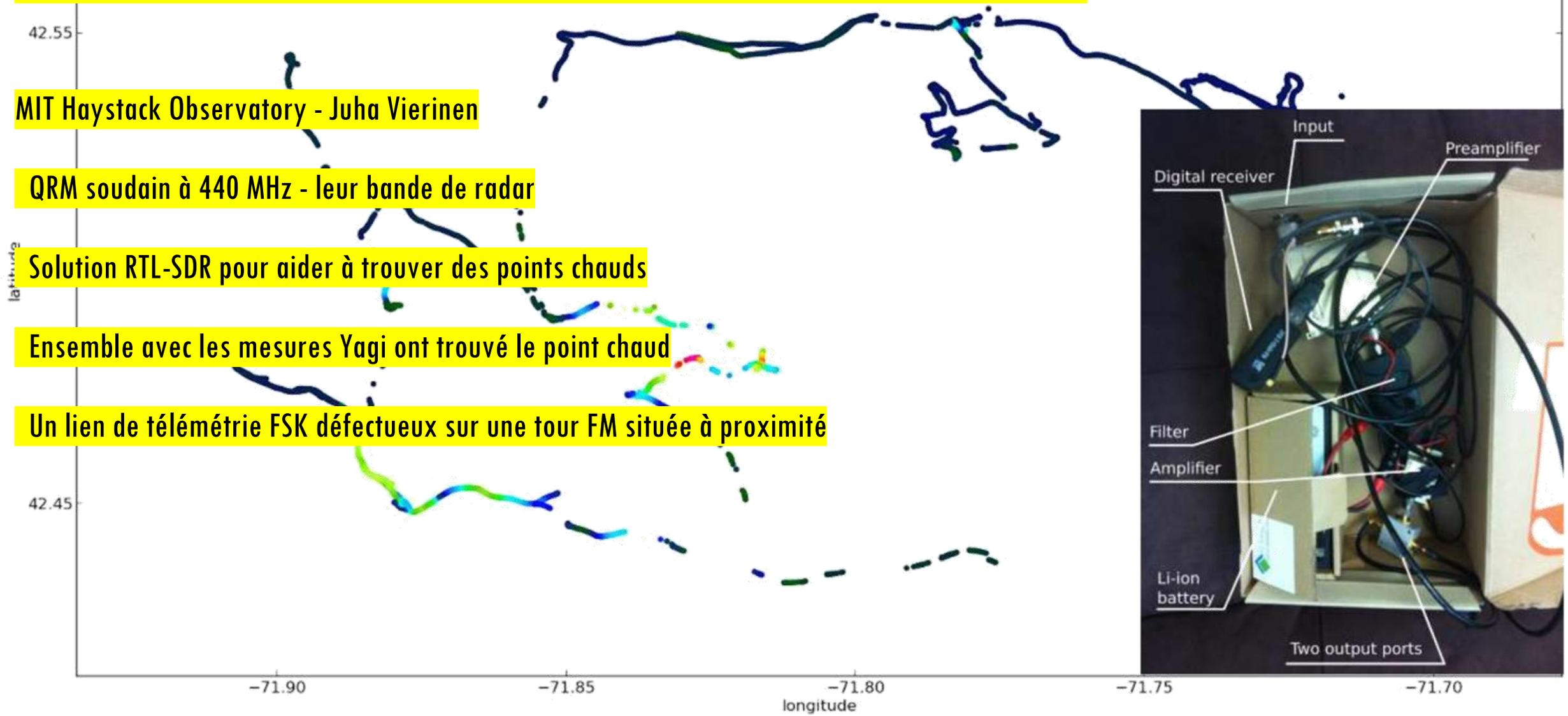
MIT Haystack Observatory - Juha Vierinen

QRM soudain à 440 MHz - leur bande de radar

Solution RTL-SDR pour aider à trouver des points chauds

Ensemble avec les mesures Yagi ont trouvé le point chaud

Un lien de télémétrie FSK défectueux sur une tour FM située à proximité



PLAYSTATION 3 INVESTISSEMENT REVERSE DE L'INGÉNIEUR

Les hackers veulent des consoles de jeu 'Jailbreak'
Permet l'installation de logiciels personnalisés

Jeux personnalisés, etc.

Raccorder l'entrée de l'antenne RTL-SDR entre le châssis et le sol réel (tiges de terre) RTL-SDR reçoit le bruit de la CPU

Peut essayer de décoder les instructions du CPU du bruit. Jamais été très loin dans le processus d'ingénierie inverse
Les méfaits du procès

INGÉNIERIE REVERSE UN DEFIBRILLATEUR CARDIAQUE IMPLANT

ICE - Défibrillateur cardiaque implanté

Protège les patients susceptibles d'arythmie, de fibrillations et de troubles cardiaques anormaux en surveillant et choquant.

ICeeData - Projet d'ingénierie inverse et de surveillance des données de télémétrie sans fil Pourquoi?

Les données sont transférées par le biais de la bande ISM sans fil à l'internet 3G au bureau des médecins.
Mais seulement disponible pour consultation au bureau des médecins.

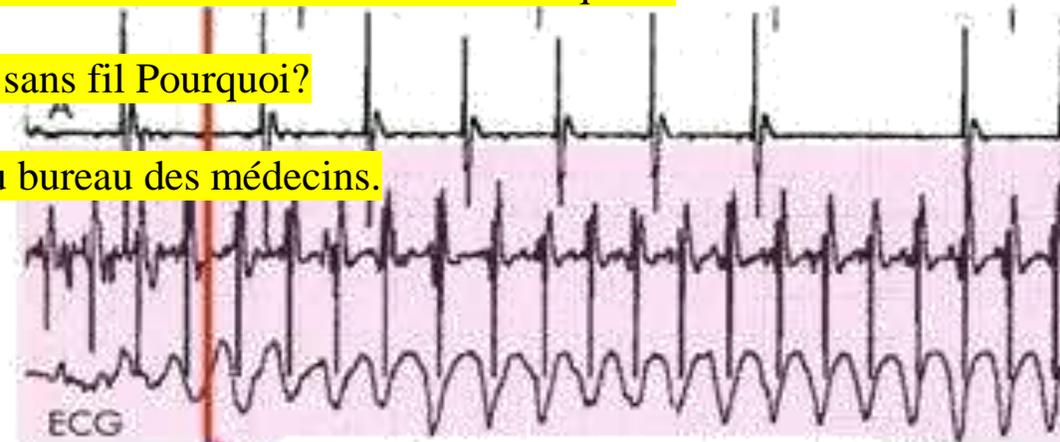
Habituellement, les rendez-vous sont une fois par an ou moins

Le patient devrait avoir accès à ces données tout le temps

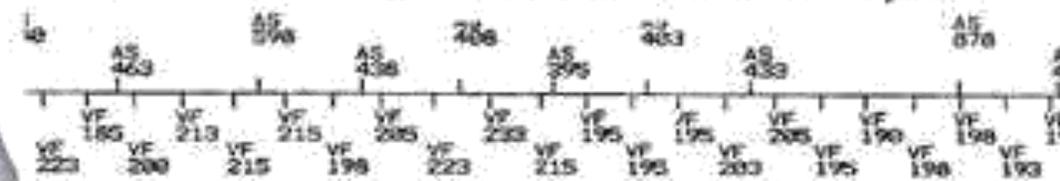
Aide à faire de meilleurs choix de style de vie

"...the ICD sense
and delivers a high
energy shock to restore normal rhythm.
Patients will feel a thump to the chest
when a ICD shock is delivered"

VF is sensed by the ICD lead and a shock is delivered



ICD Shock restores Normal Rhythm



MONITEUR GLOBAL NETWORKED

modify.

track cube sats
and be imaginative

Bigwhoop - réseau de récepteurs radio RTL-SDR à large spectre

Le réseau planifie automatiquement l'écoute et la collecte de données

Concentrez-vous sur les expériences scientifiques, les exemples incluent
Trouver des spots silencieux pour les radiotélescopes

Collecte de données satellitaires LEO

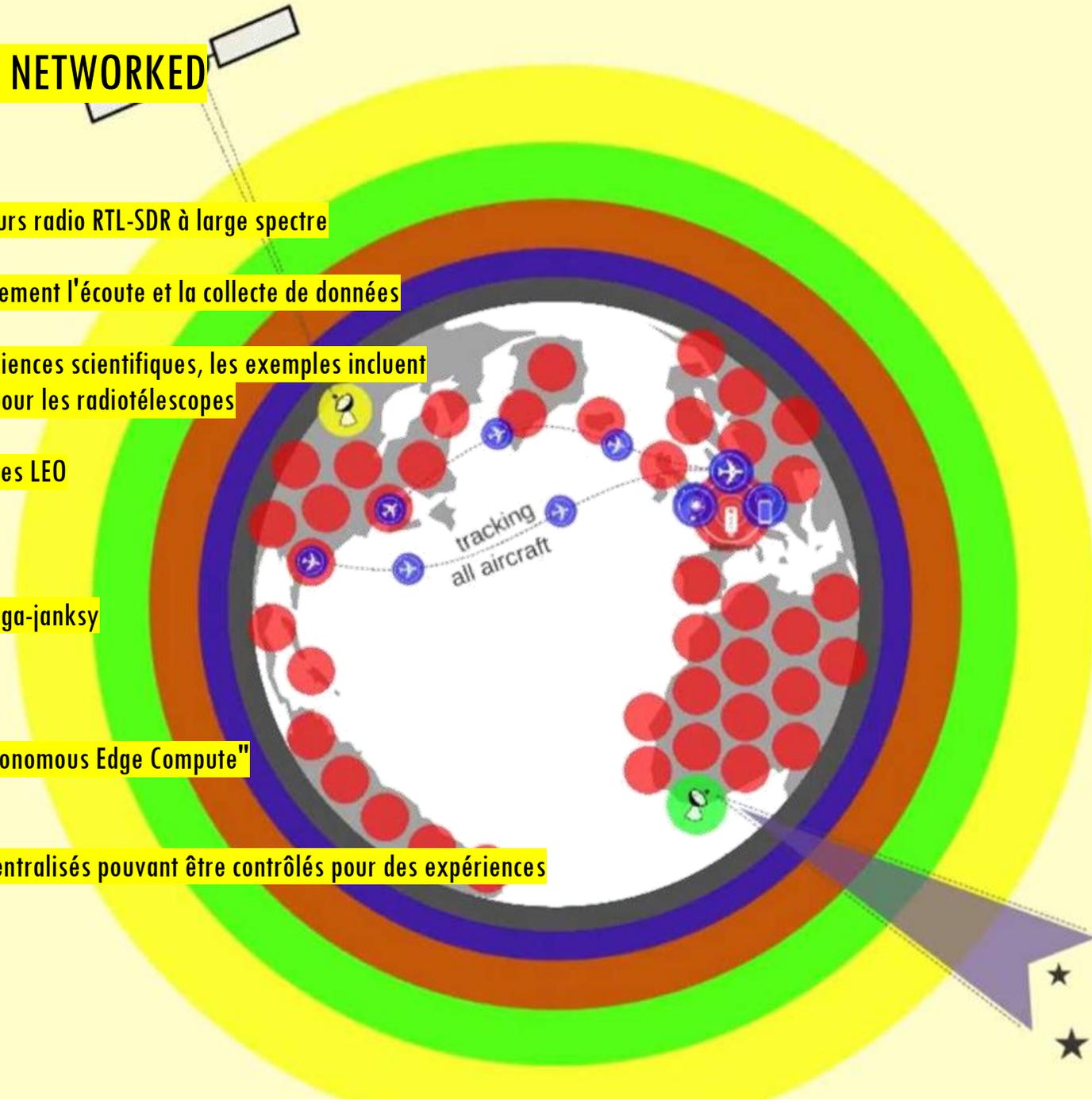
Surveillance du spectre

Radio astronomie: éclats de Giga-jansky

IBM "Horizon décentralisé Autonomous Edge Compute"

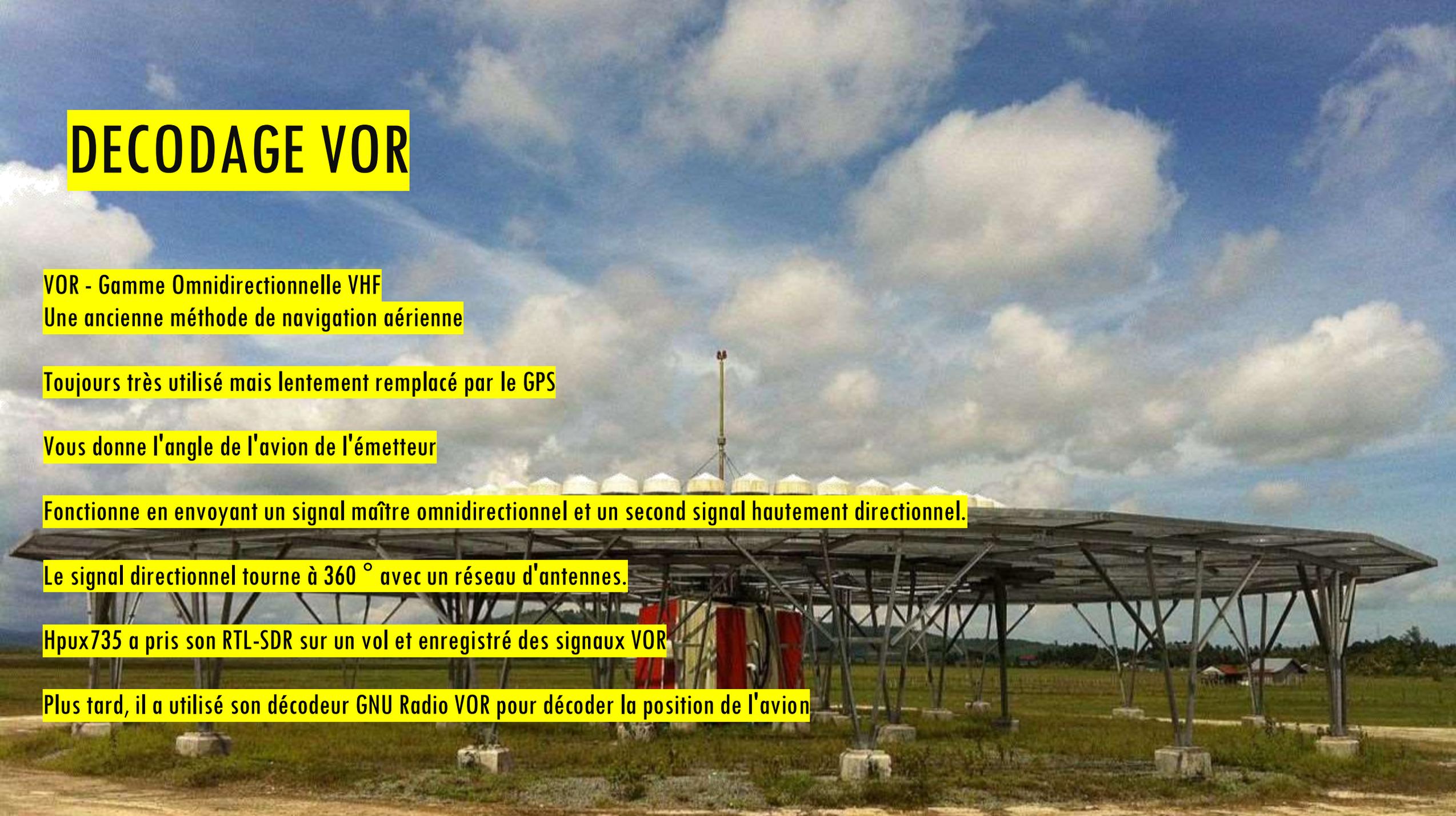
Semblable à la grande idée

Des centaines de RTL-SDR décentralisés pouvant être contrôlés pour des expériences



...or finding
sweet spots for
radio telescopes.

DECODAGE VOR



VOR - Gamme Omnidirectionnelle VHF

Une ancienne méthode de navigation aérienne

Toujours très utilisé mais lentement remplacé par le GPS

Vous donne l'angle de l'avion de l'émetteur

Fonctionne en envoyant un signal maître omnidirectionnel et un second signal hautement directionnel.

Le signal directionnel tourne à 360° avec un réseau d'antennes.

Hpux735 a pris son RTL-SDR sur un vol et enregistré des signaux VOR

Plus tard, il a utilisé son décodeur GNU Radio VOR pour décoder la position de l'avion

JUPITER NOISE BURSTS

Écouter des éclats de bruit entre 20 et 40 MHz provenant de la planète Jupiter

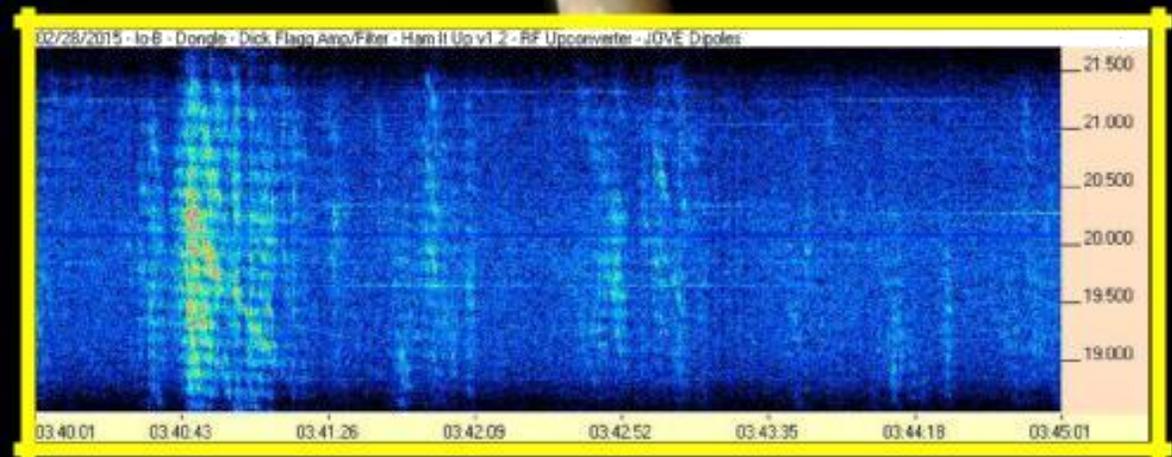
Crée des "orages de bruit radio" à travers une relation orbitale complexe entre Jupiter
Et sa lune volcanique Io.

Qu'avez-vous besoin pour recevoir le bruit de Jupiter?

Antenne: un simple dipôle réglé à environ 20 MHz fonctionnera

Filtre + LNA

Toute radio comme RTL-SDR



Tire Pressure Monitoring System for iPhone



DONNÉES TPMS SUR LE PNEU

TPMS - Système de surveillance de la pression des pneus

Transmet sans fil les données de la pression des pneus vers un tableau de bord dans la voiture

Placez un capteur par pneu

Peut facilement recevoir et décoder les données avec un RTL-SDR

Problème de sécurité?

Chaque capteur possède un identifiant unique

Peut-être suivre les véhicules à travers la ville

EN DIRECT DES DONNÉES DU COCKPIT ADS-B

- TomL's RTL1090XHSI

- Utilisez des données ADS-B en direct pour créer une expérience de cockpit authentique

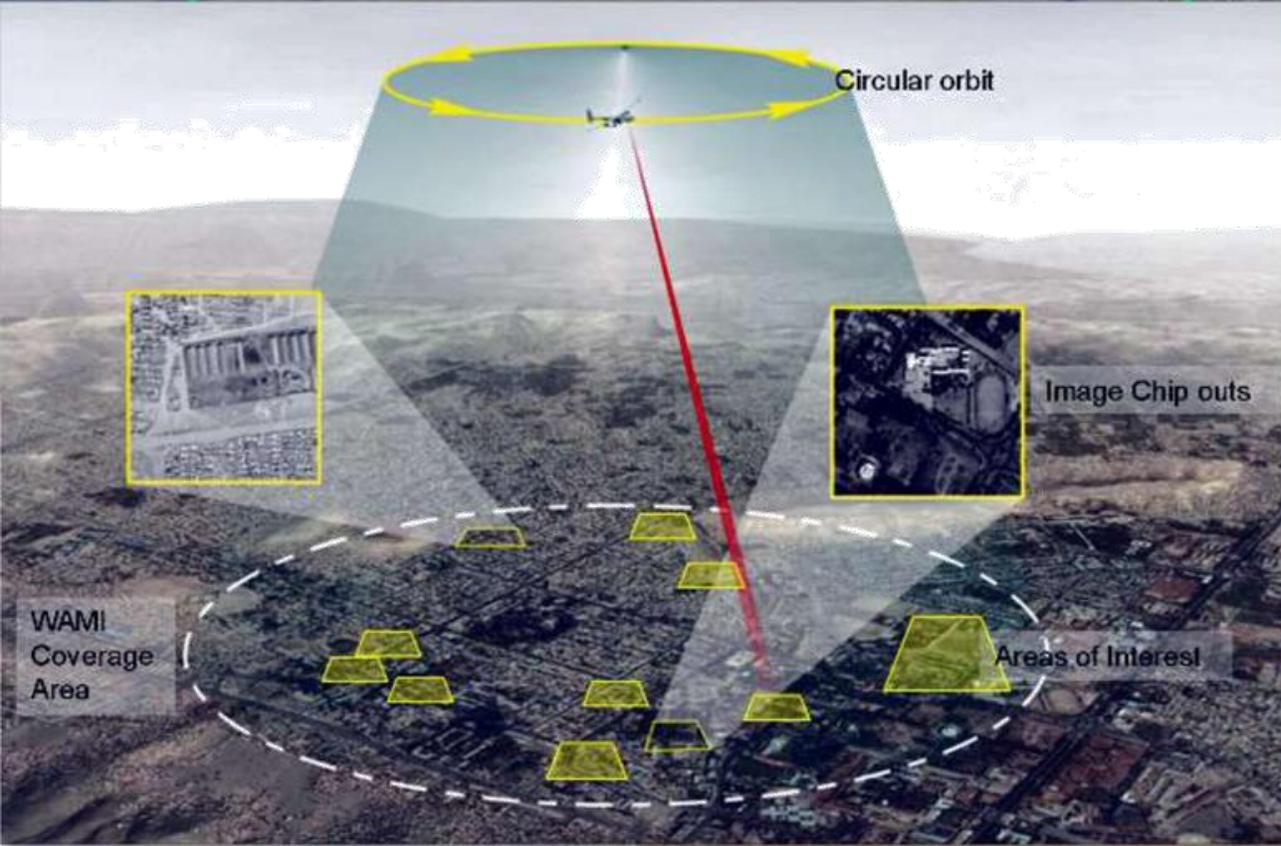
- Basé sur un logiciel de simulation de vol

- Faites attention lors de l'utilisation sur un avion réel

- Ne paniquez pas les gens



VOIR LES WATCHMEN AVEC ADS-B



Surveillance persistante de grande envergure

Systèmes de surveillance persistants à Dayton, OHIMSI Catchers

Permet aux autorités d'écouter les téléphones cellulaires

John Wiseman @lemonodor remarque des avions suspects circulant pendant des jours après les émeutes de Baltimore.

Il a 6 mois de billes ADS-B de son RTL-SDR

En cherchant les codes de squawk, il trouve plusieurs vols similaires dans ses journaux.

Tous les inscrits généreusement nommés faux entreprises.

Le FBI confirme plus tard que ce sont leurs avions

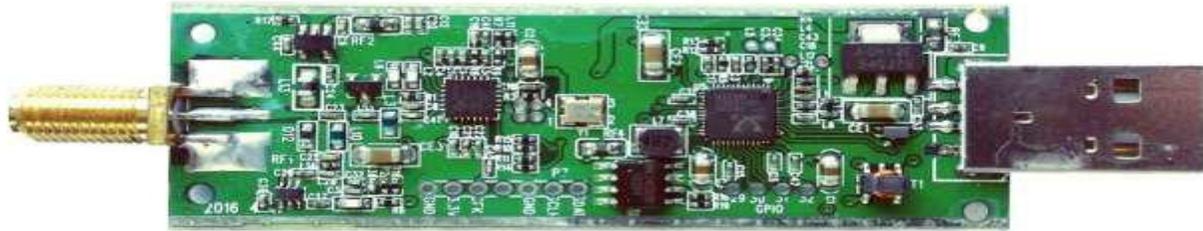
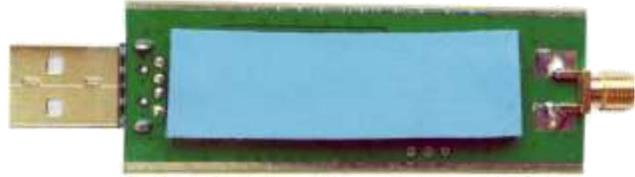
Très probablement, une surveillance de grande envergure

SATELLITES MORT: METEOR M-N1

Ressuscité après avoir été désaffecté

Un peu brisé, semble tomber
Peut souvent voir le bord de la terre

Maintenant éteint à nouveau



REDESIGNED RTL-SDR V3

Problèmes avec les dongles "génériques"

1. oscillateur dériveur (fréquence instable)
2. Aucun blindage
3. De nombreuses éperons
4. Problèmes avec la réception de la bande L
5. Connecteur radio MCX peu fréquent

RTL-SDR.com V3 corrige et ajoute des fonctionnalités

1. Oscillateur TCXO
2. Blindage métallique
3. PCB redessiné et filtrage de bruit supplémentaire
4. Réchauffeur thermique pour casque métallique
5. Connecteur SMA
6. Tee de partialité
7. Réception HF par prélèvement direct

DÉCODAGE DES BALONS MÉTÉOROLOGIQUES

Deux fois par jour, les ballons météorologiques se lancent dans de nombreux endroits

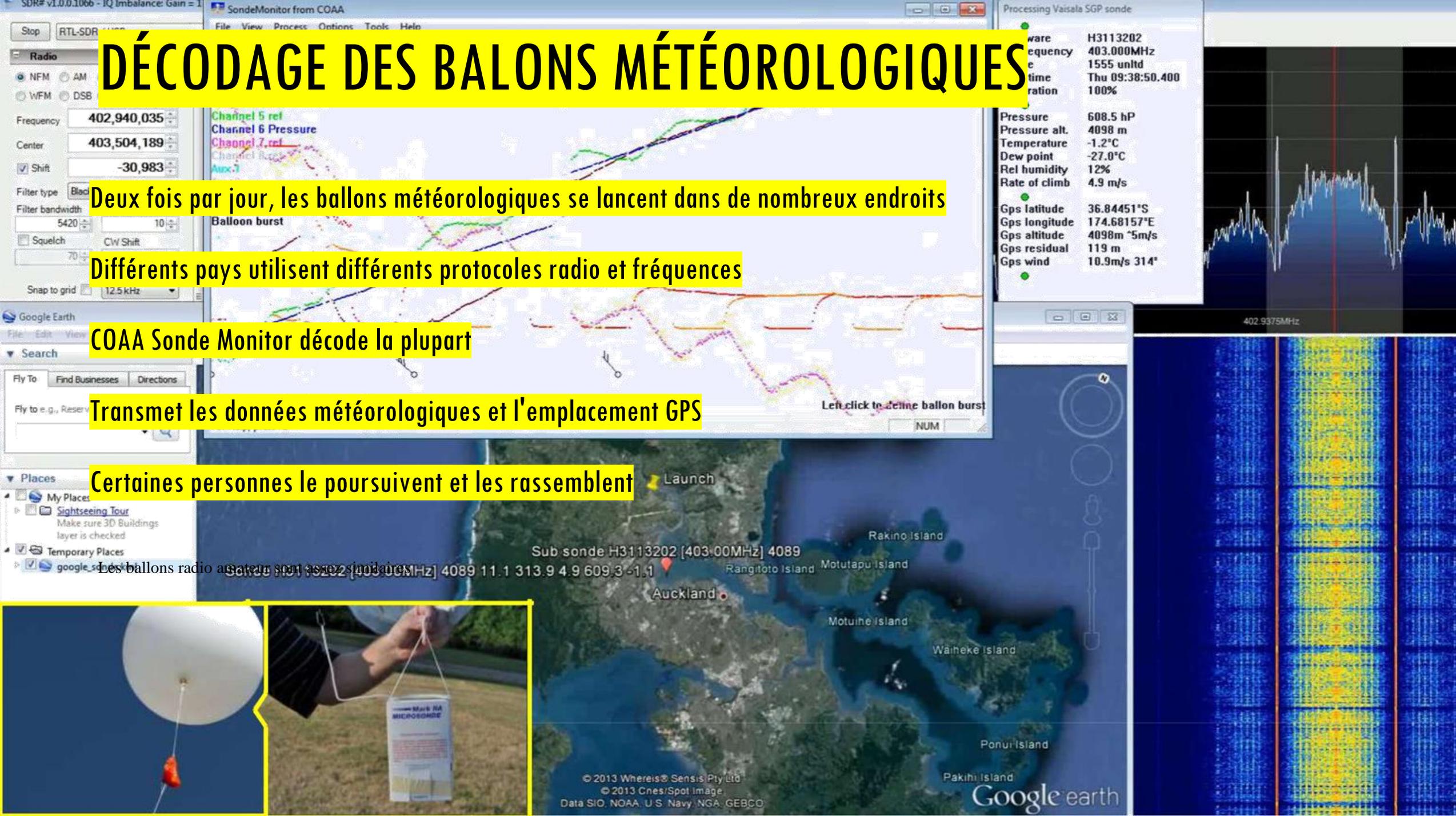
Différents pays utilisent différents protocoles radio et fréquences

COAA Sonde Monitor décode la plupart

Transmet les données météorologiques et l'emplacement GPS

Certaines personnes le poursuivent et les rassemblent

Les ballons radio amateur sont assez similaires



Pressure	608.5 hPa
Pressure alt.	4098 m
Temperature	-1.2°C
Dew point	-27.0°C
Rel humidity	12%
Rate of climb	4.9 m/s
Gps latitude	36.84451°S
Gps longitude	174.68157°E
Gps altitude	4098m ±5m/s
Gps residual	119 m
Gps wind	10.9m/s 314°

Sub sonde H3113202 [403.00MHz] 4089
Sonde H3113202 [403.00MHz] 4089 11.1 313.9 4.9 609.3 -1.1

Google earth

CARACTÉRISTIQUES DU FILTRE DE MESURE ET ANTENNE VSWR

RTL-SDR en tant qu'analyste de réseau

Mesurer les caractéristiques du filtre

Mesurer les talons coaxiaux

Mesurer l'antenne VSWR

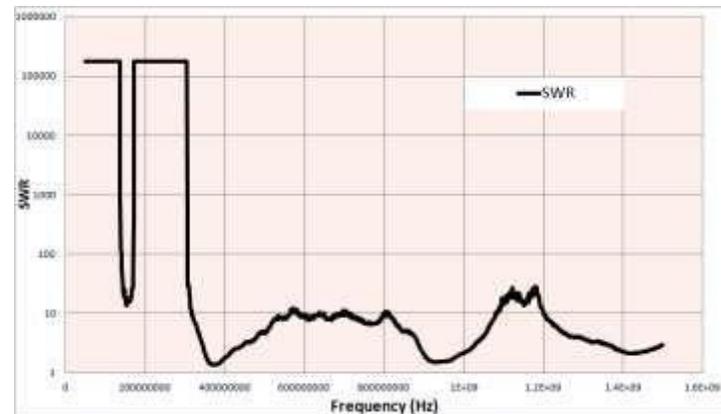
Pas totalement précis, mais vous donne une lecture assez bonne.

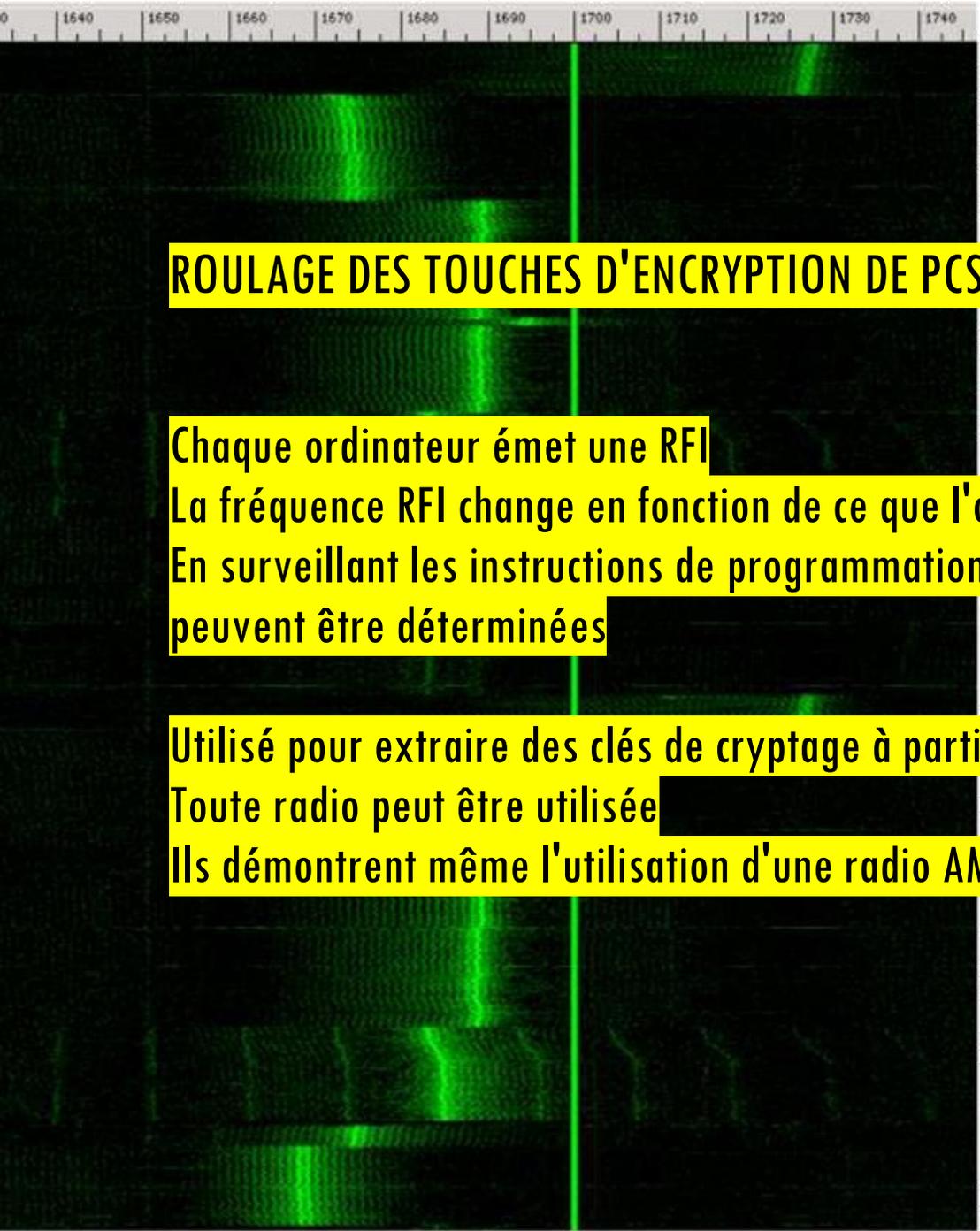
De quoi avez-vous besoin:

RTL-SDR

Source de bruit à large bande

Coupleur directionnel





ROULAGE DES TOUCHES D'ENCRYPTION DE PCS

Chaque ordinateur émet une RFI
La fréquence RFI change en fonction de ce que l'ordinateur fait
En surveillant les instructions de programmation d'assemblage RFI peuvent être déterminées

Utilisé pour extraire des clés de cryptage à partir d'un PC
Toute radio peut être utilisée
Ils démontrent même l'utilisation d'une radio AM de poche

MUL
FMUL
ADD
MEM
NOP
HLT



COMMENT RECEVOIR CES SATELLITES

MÉTÉOROLOGIQUES

Ils sont en "orbite terrestre basse"
Près de la terre, mais orbite assez rapidement

Chaque passe sera d'environ 10 minutes

Besoin d'une antenne satellite (rayonnement des rayons vers le ciel)

QFH

Tourniquet

V-Dipôle

Utilisez un logiciel comme Orbitron pour
suivre les satellites



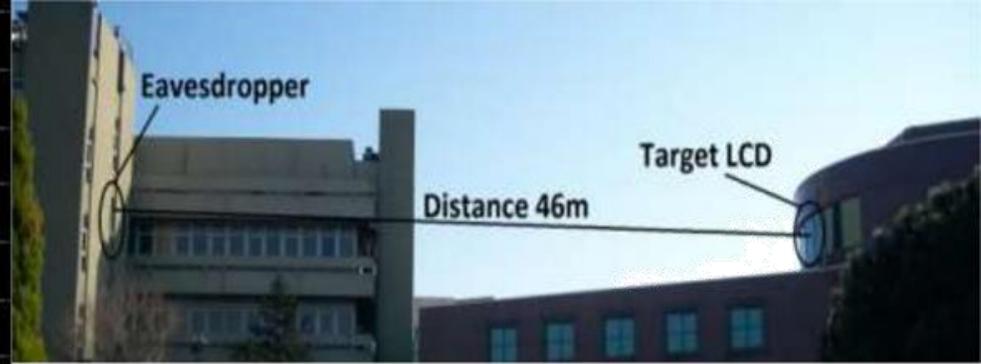
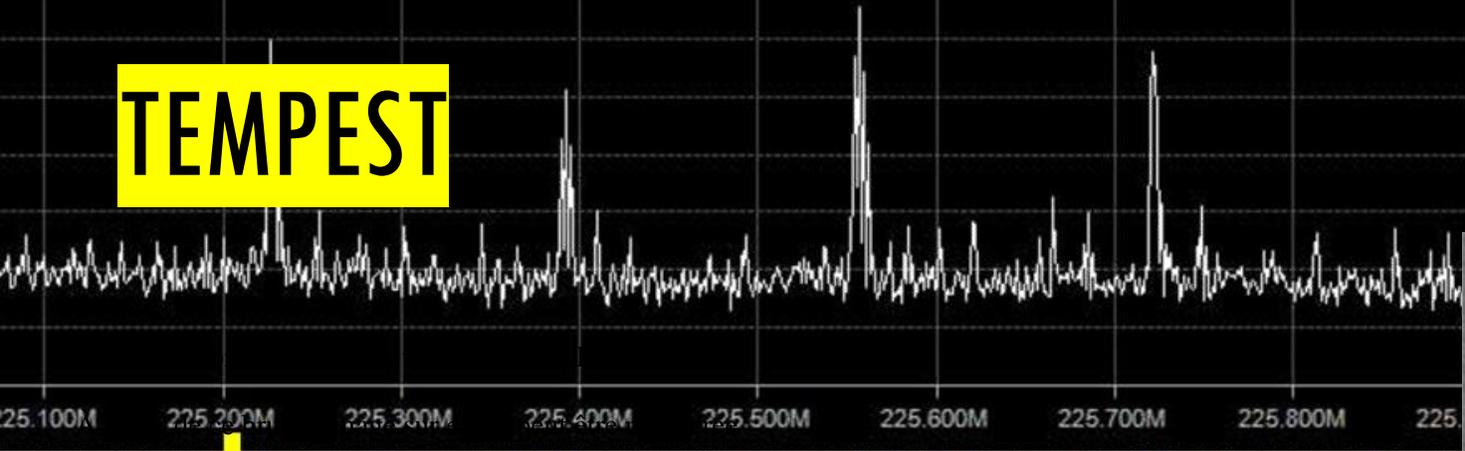
NOAA 15

METEOR-M 1

+ Auckland

NOAA 19

TEMPEST



```
de_DE.UTF-8 German | Deutsch  
es_ES.UTF-8 Spanish | Español  
fr_FR.UTF-8 French | Français  
it_IT.UTF-8 Italian | Italiano  
ja_JP.UTF-8 Japanese | 日本語  
pt_BR.UTF-8 Brazilian Portuguese | Português do Brasil  
ru_RU.UTF-8 Russian | Русский  
zh_CN.UTF-8 Chinese (Simplified) | 简体中文  
zh_TW.UTF-8 Chinese (Traditional) | 正體中文 - 臺灣
```

Logiciel RTL-SDR: TempestSDR

Exemple: mon LCD émet RFI à ~ 225 MHz. Les tonalités changent en fonction de ce qui se trouve sur l'écran

Utilisez SDR pour voler des clés de cryptage à partir d'un PC
Obtenir les instructions du code d'assemblage

Reverse engineer a Playstation

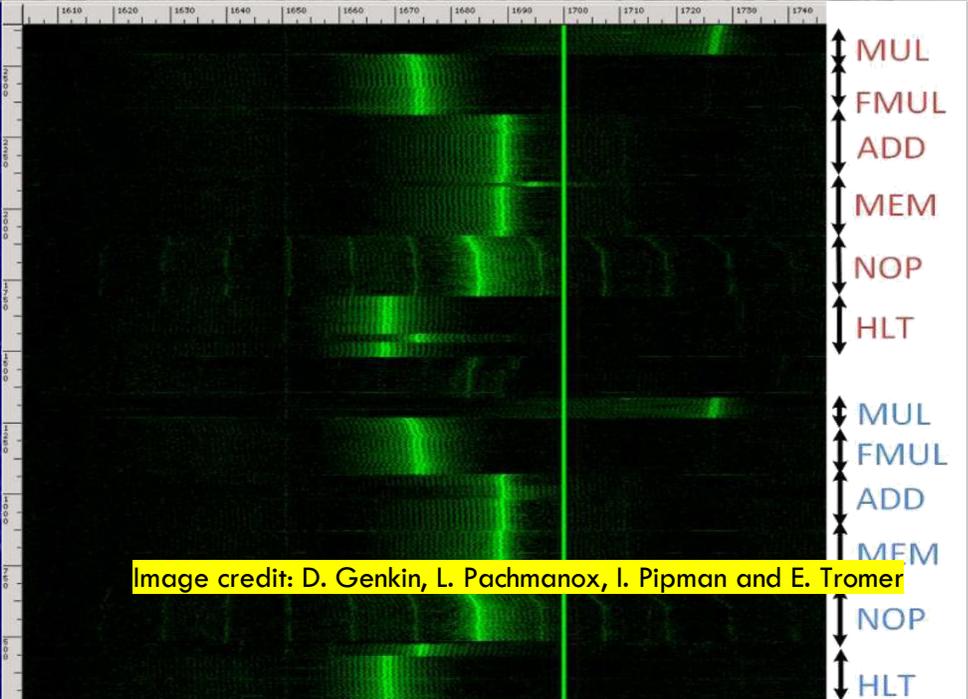


Image credit: D. Genkin, L. Pachmanox, I. Pipman and E. Tromer

SATELLITES L-BAND: INMARSAT AERO

Inmarsat AERO - La version satellite de ACARS L-band - Uplink. Contient des messages

Comme: Messages courts vers et depuis le personnel de vol

Rapports météorologiques

Plans de vol

Télémetrie

C-band - Lien descendant. Contient des informations de position de l'avion.

Sur MH370, AERO a été éteint.

Logiciel: JAERO



N13954
UA1987
37996

N13954
UA1987
37996

N809AA

N28338004
A4127
38004

N778ANA
AA175
36000

N26960
UA32
37996

N78038004
UA79

H36996
KE81
35000

N76
35000

B-5123
MU572

UA827
37000

37000

HL7628
KE122
37996

N779UA
UA201
36000

N213UA
UA2177
41000

N215UA
UA218
35000

N380HA
HA12
41000