2025 ACM Wireless Risks Analysis Presentation

Joseph Jesson
CEO RFSigint Group
jejesson4@gmail.com

https://www.britishpoles.uk/how-the-polish-mathematicians-deciphered-and-handed-over-the-enigma-code-to-french-and-british-allies/

2025 ACM Wireless Risks Analysis Presentation

- Communications SOC Supply Risks Analysis

- IoT Security and Spectrum Window

- Aircraft Digital Communication Risks

- Drone Detection and Identification

Joseph Jesson
CEO RFSigint Group
jejesson4@gmail.com

https://www.britishpoles.uk/how-the-polish-mathematicians-deciphered-and-handed-over-the-enigma-code-to-french-and-british-allies/

QUECTEL RISK MITIGATION

1. **Qualcomm MDM9205 license**, identical chip set in **Quectel BG95**, Telit 910, and now Thales (Cinterion) EXS62

2. **COI = Made in Germany** (Siemens – Leesys – in Liptzieg), OR

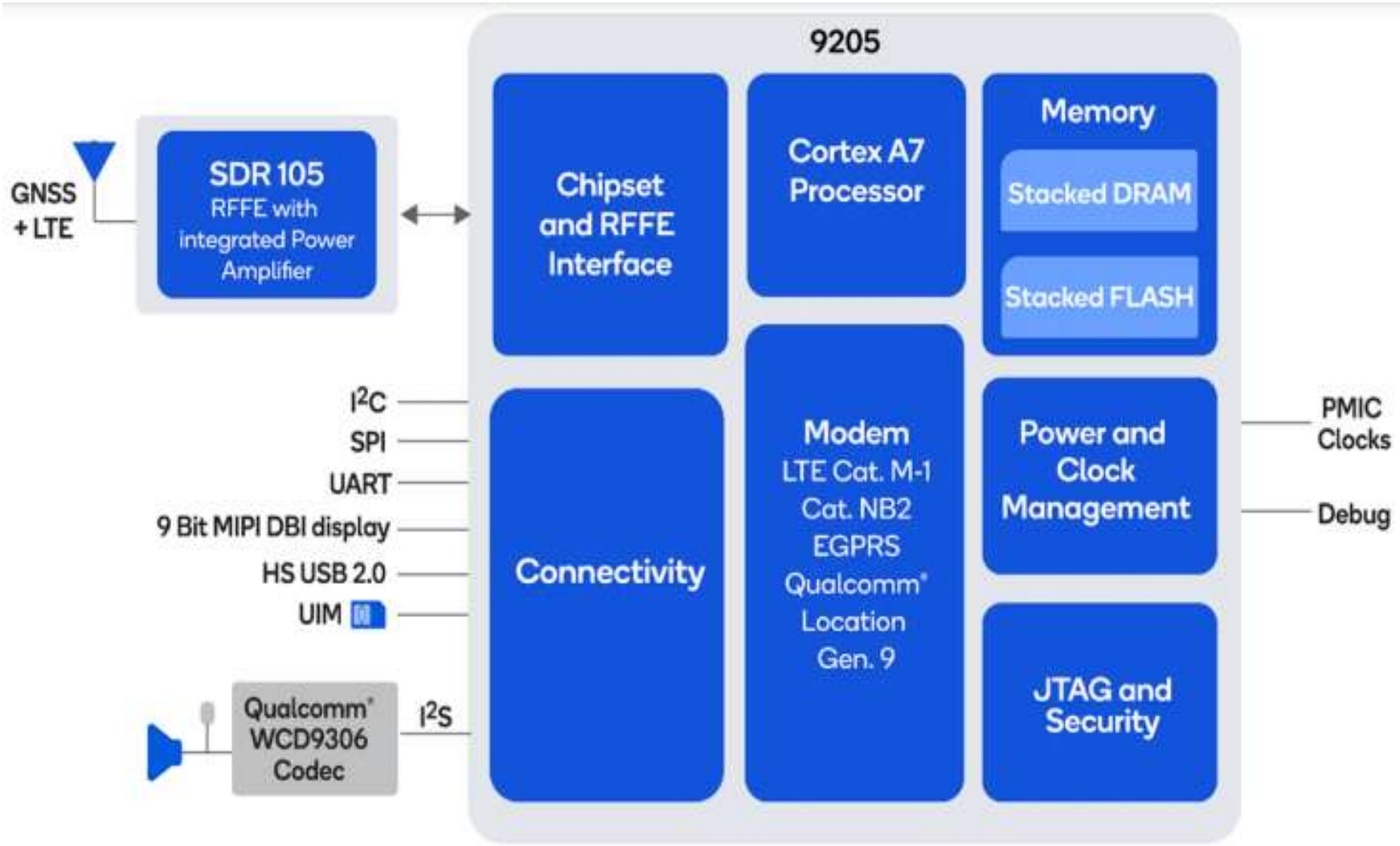
3. **COI = Made in USA ,** OR COI = Taiwan, China, Vietnam

4. **Production Lead Times of 8 Weeks**

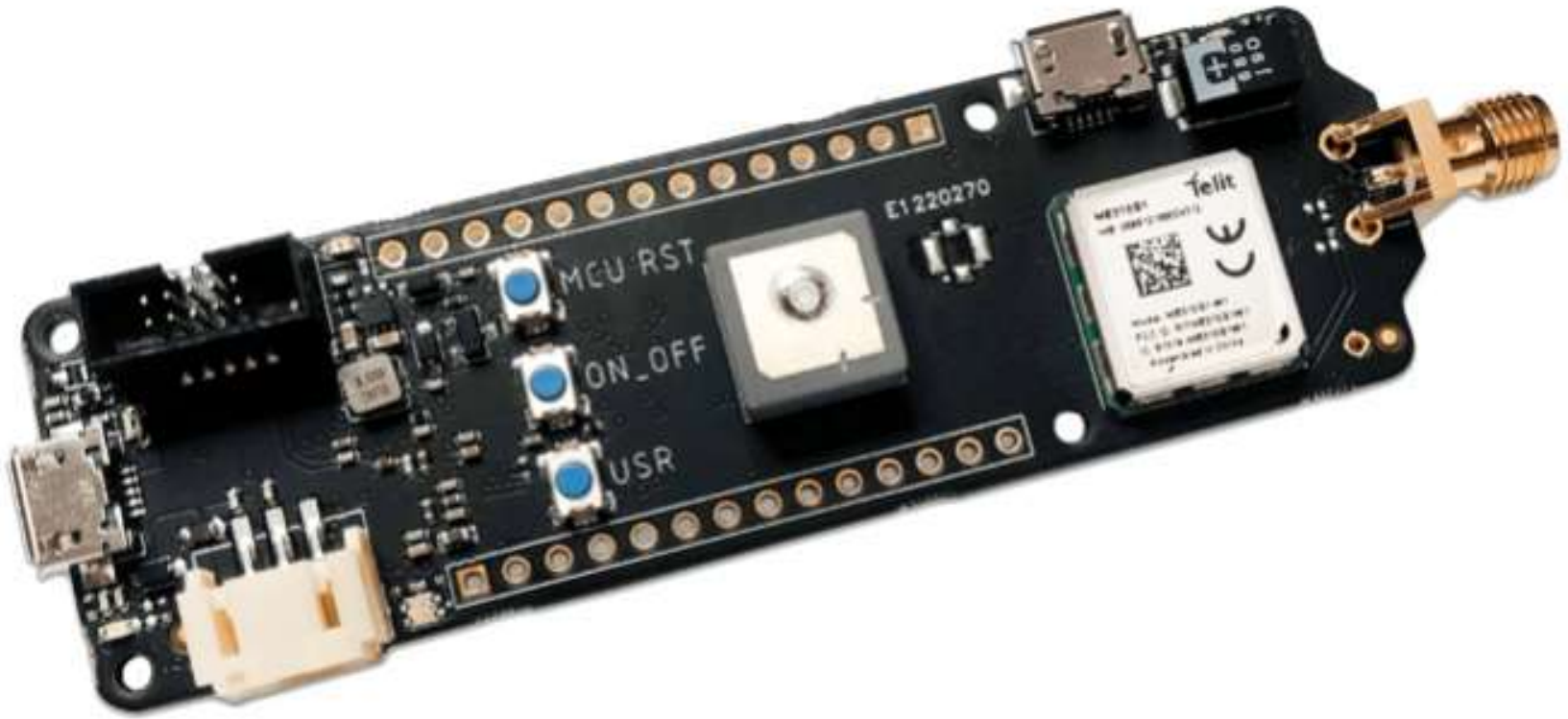
5. **Interested in also quoting package Contract Mfg**

6. **Quectel's BG95 AT commands vs. Thales (Cinterion) EXS62**

QUALCOMM 9205 LTE Modem CS Architecture

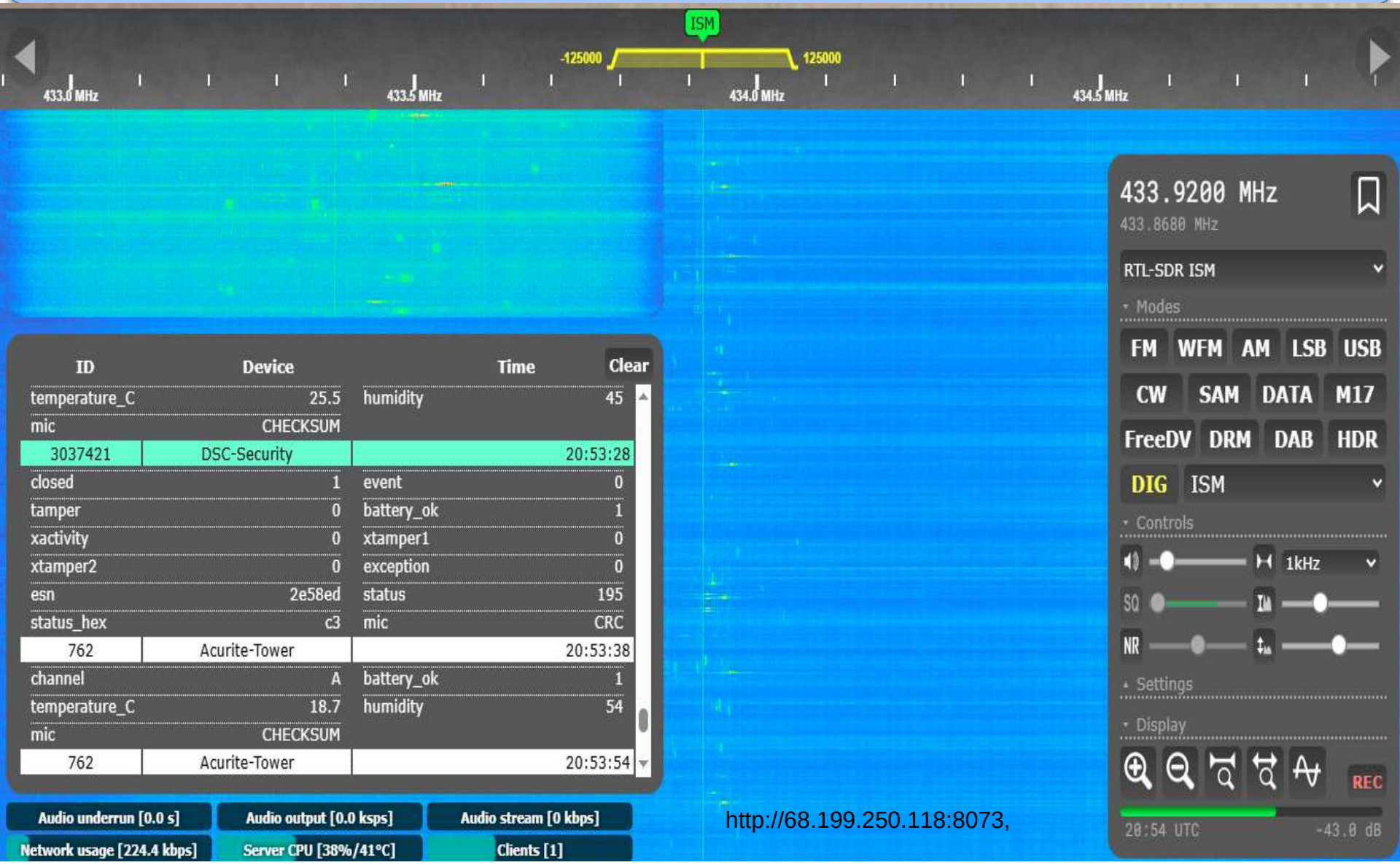


TELIT ME910G1-WW Development Board



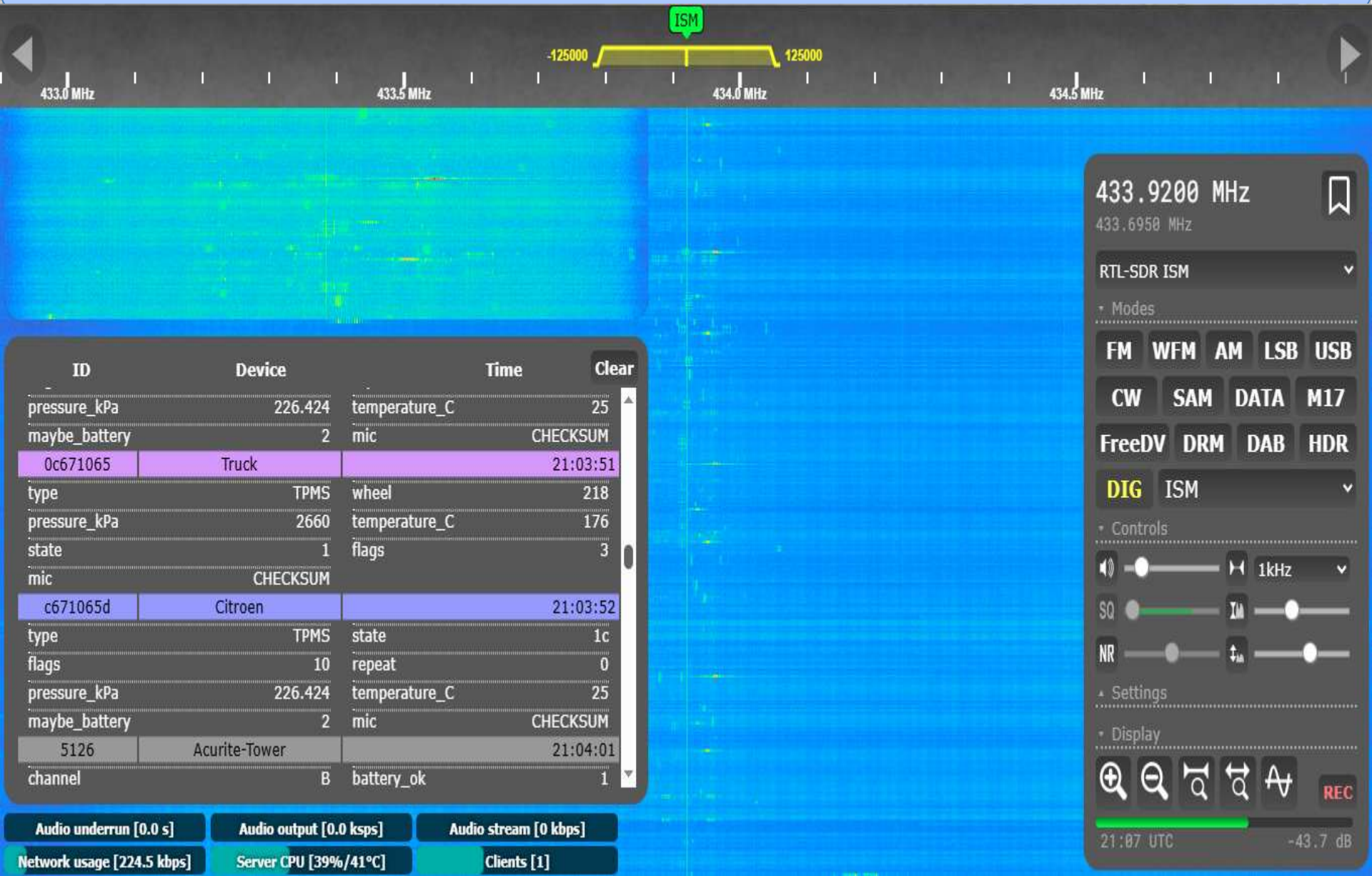
Mounts ME310G1-WW module with **LTE Cat M1/NB1 , GNSS receiver**.
MKR form factor that features a low-power **ARM® Cortex®-M0 32-bit SAMD21 microprocessor**.
Bosch Sensortec BMA400 triaxial acceleration sensor, 12-bit resolution and typical µA current.
Full compatibility with the standard's software development environment.

Internet of Things
433MHz ISM Spectrum
Weather Tower and Security Station



http://68.199.250.118:8073,

Internet of Things
433MHz ISM Spectrum
Citroen Automobile Start



December 11, 2024, New Jersey

12/11/2024

NJ Congressman Jeff Van Drew announced December 11th, 2024 that drones over NJ are from an Iranian "mothership" stationed off the U.S. East Coast, reportedly launching drones now flying over New Jersey.

Finally, on January 29th, the President announced, "The drones that were flying over New Jersey in large numbers were authorized to be flown by the FAA for research and various other reasons … this was not the enemy,"

Pentagon's Response

"Maj. Gen. Pat Ryder, the Pentagon press secretary, said the military was providing "active and passive detection capabilities" and "counter-drone capabilities" to Picatinny Arsenal and Naval Weapons Station Earle." The Pentagon sent counter-drone weapons from the corporation, dzyne.com

Pentagon’s Response

HANDHELD | WEARABLES

DRONEBUSTER® DTIM KIT

Detect, Track, Identify, Mitigate

Now available: Dronebuster® 4-EU – a region-specific, wearable counter-UAS solution engineered for European frequency compliance and mission-critical drone defense.

Dronebuster® DTIM Kit:

Detects drones up to 7 km away

Effective jamming and optional PNT (Position, Navigation, Timing) attack mode

---

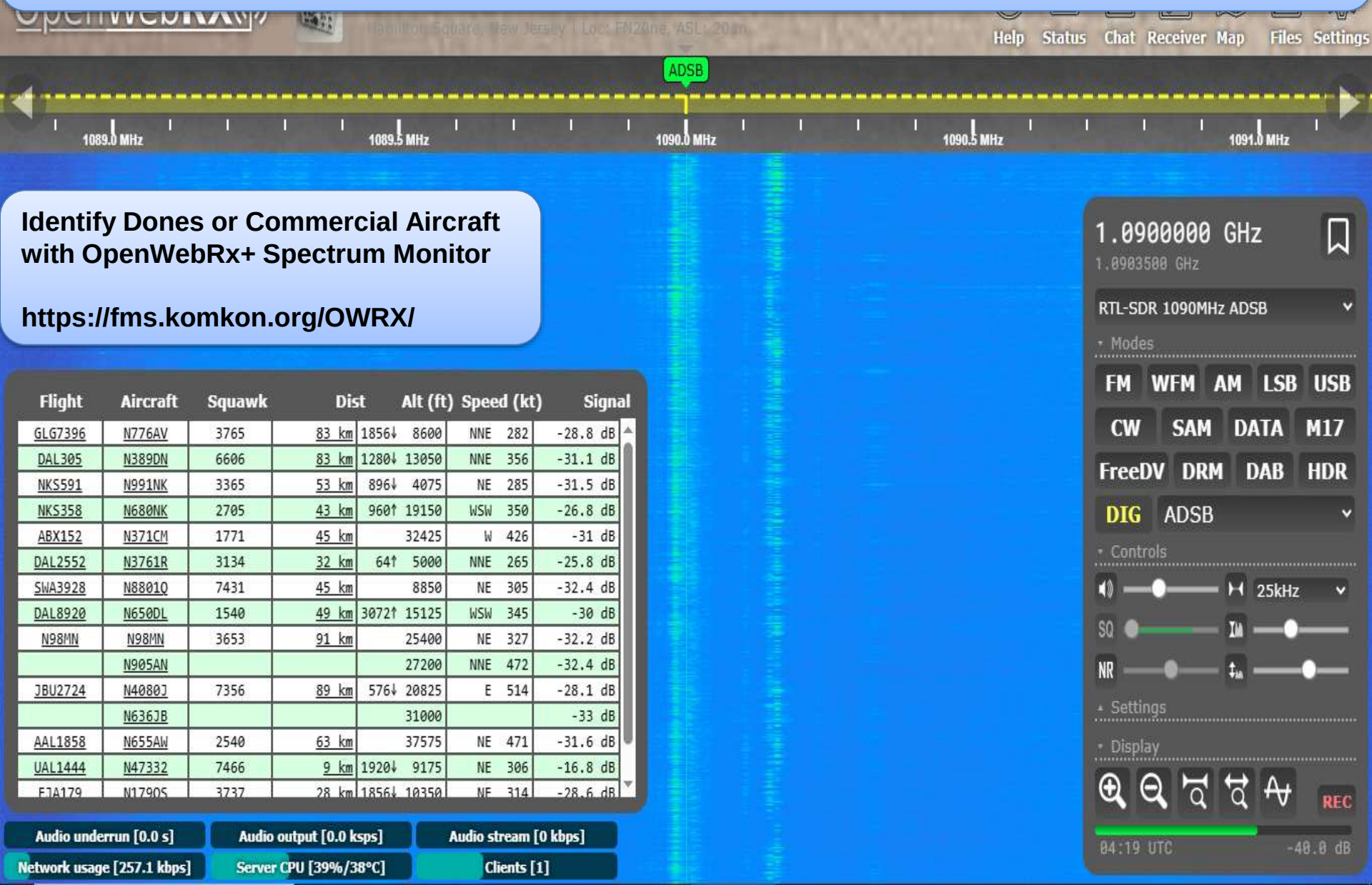
Lightweight, wearable, and **ATAK-compatible** for seamless situational awareness

---

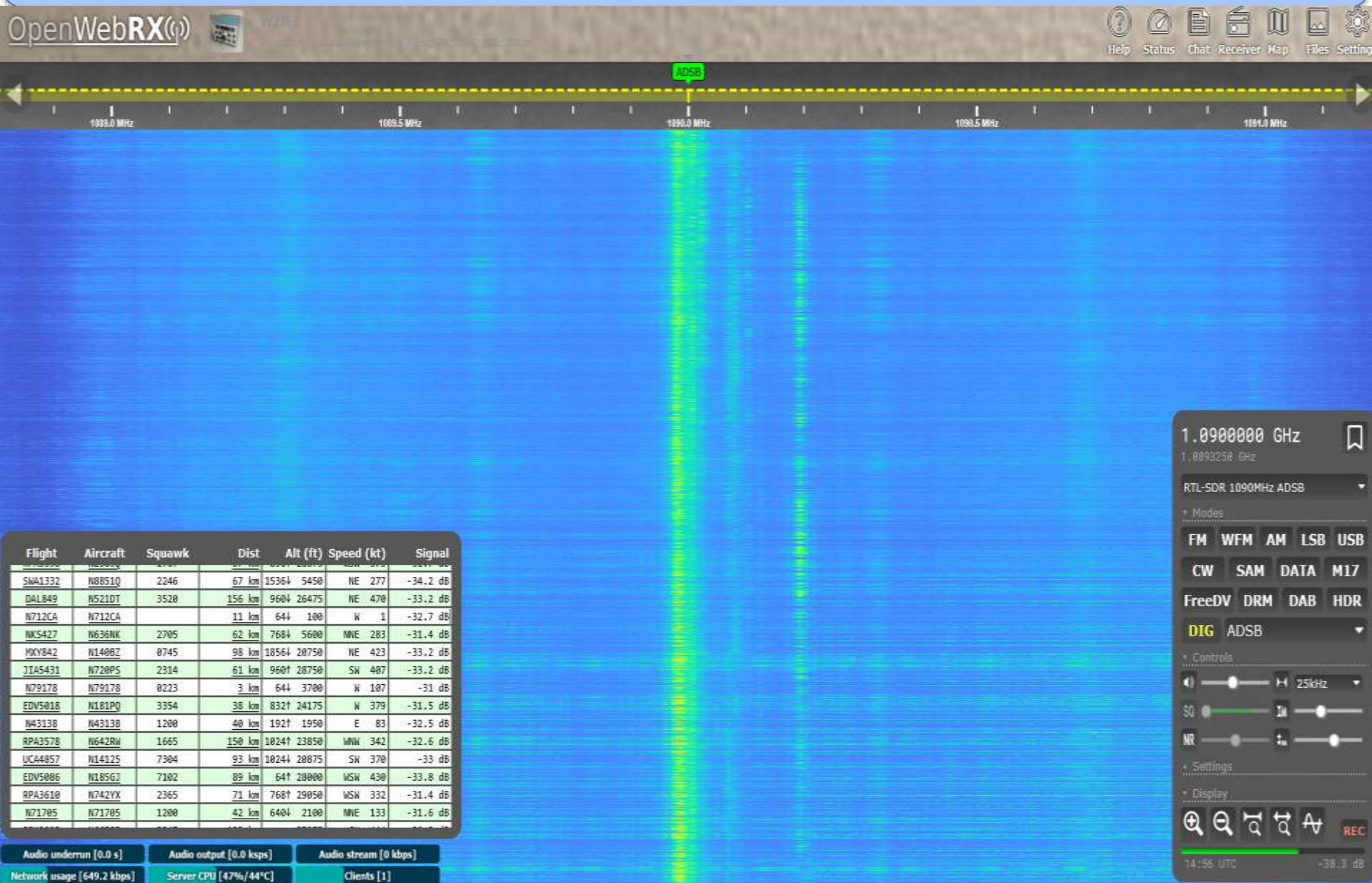
Handheld, mobile, and fixed-site configurations available for layered defense

---

Automatic Dependent Surveillance - Broadcast (ADS-B) is an advanced surveillance technology that combines an aircraft's positioning source, aircraft avionics, and a ground infrastructure

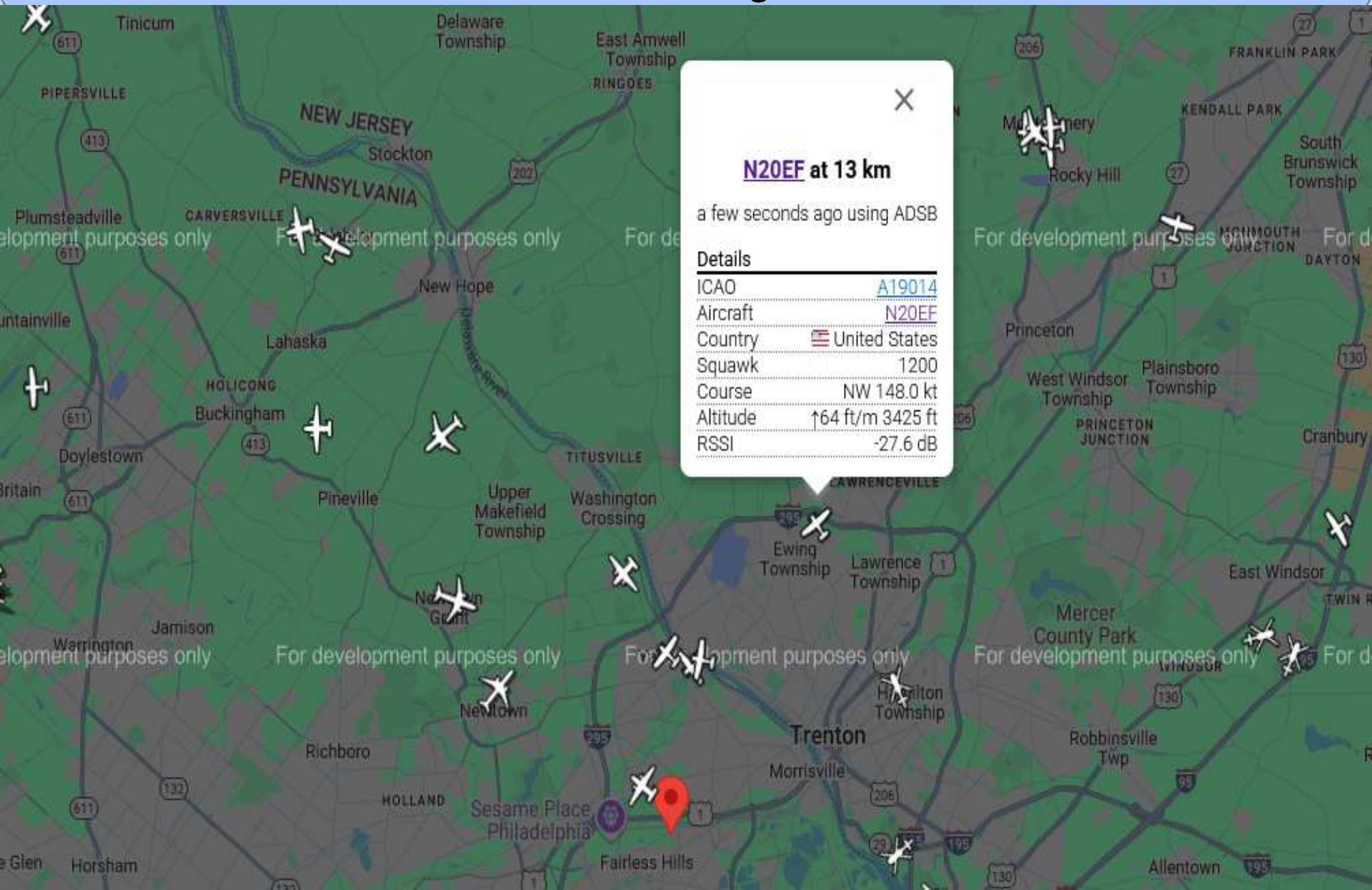


Automatic Dependent Surveillance - Broadcast (ADS-B) is an advanced surveillance technology that combines an aircraft's positioning source, aircraft avionics, and a ground infrastructure

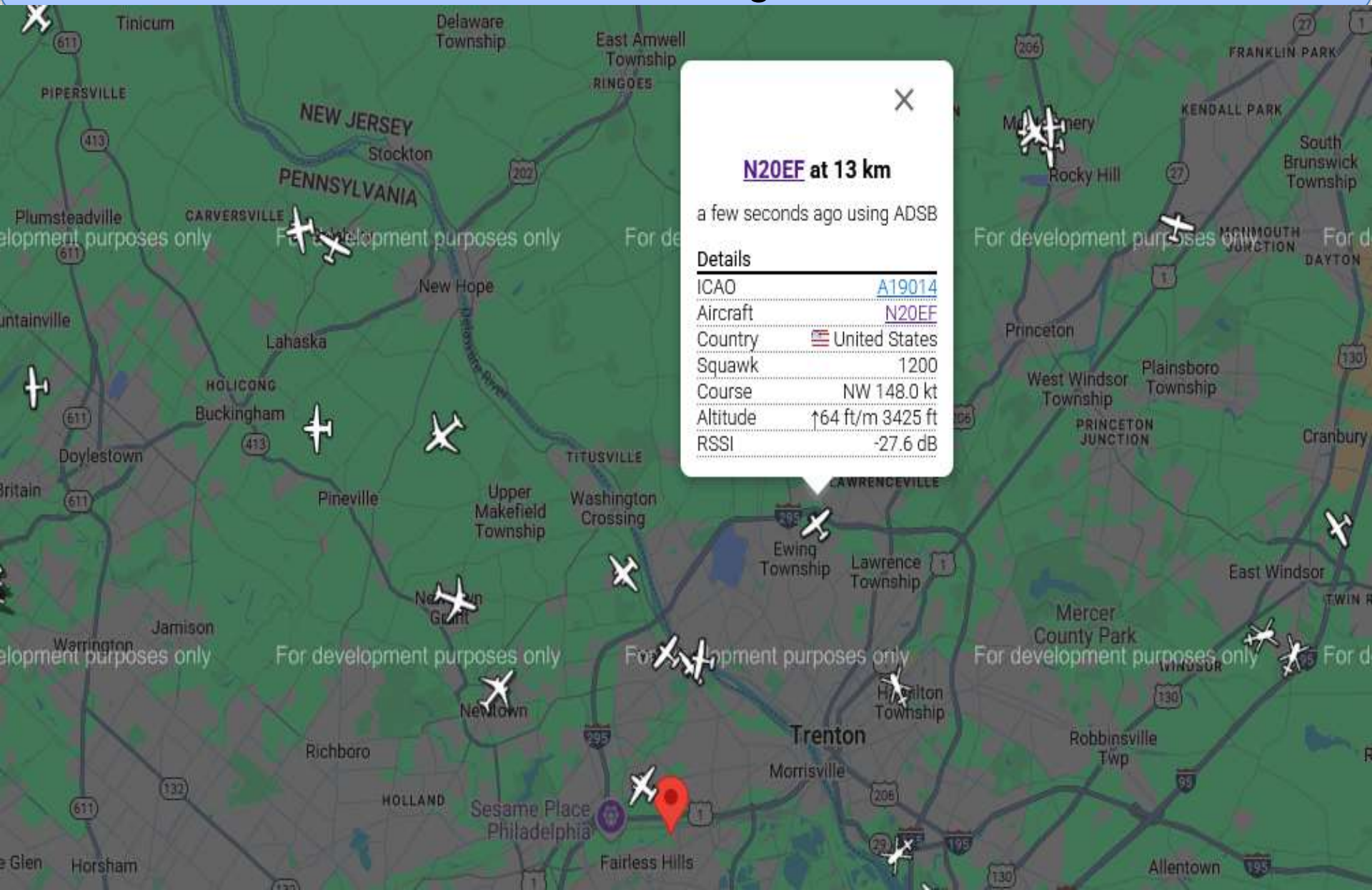


Flight	Aircraft	Squawk	Dist	Alt (ft)	Speed (kt)	Signal
SWA1332	N8851Q	2246	67 km	15364 5450	NE 277	-34.2 dB
DAL849	N521DT	3520	156 km	960↓ 26475	NE 470	-33.2 dB
N712CA	N712CA		11 km	64↓ 100	W 1	-32.7 dB
NKS427	N636NK	2705	62 km	7684 5600	NNE 283	-31.4 dB
MXY842	N140BZ	0745	98 km	18564 20750	NE 423	-33.2 dB
JIA5431	N720PS	2314	61 km	960↑ 28750	SW 407	-33.2 dB
N79178	N79178	0223	3 km	64↓ 3700	W 107	-31 dB
EDV5018	N181PQ	3354	38 km	832↑ 24175	W 379	-31.5 dB
N43138	N43138	1200	40 km	192↑ 1950	E 83	-32.5 dB
RPA3578	N642RW	1665	150 km	1024↑ 23850	WNW 342	-32.6 dB
UCA4857	N14125	7304	93 km	1024↓ 20875	SW 370	-33 dB
EDV5086	N185GJ	7102	89 km	64↑ 28000	WSW 430	-33.8 dB
RPA3610	N742YX	2365	71 km	768↑ 29050	WSW 332	-31.4 dB
N71705	N71705	1200	42 km	6404 2100	NNE 133	-31.6 dB

Automatic Dependent Surveillance - Broadcast (ADS-B) is an advanced surveillance technology that combines an aircraft's positioning source, aircraft avionics, and a ground infrastructure



Automatic Dependent Surveillance - Broadcast (ADS-B) is an advanced surveillance technology that combines an aircraft's positioning source, aircraft avionics, and a ground infrastructure



Automatic Dependent Surveillance - Broadcast (ADS-B) is an advanced surveillance technology that combines an aircraft's positioning source, aircraft avionics, and a ground infrastructure

N20EF

EN ROUTE

TTN
TRENTON, NJ
THURSDAY 01-MAY-2025
10:05AM EDT

N20EF flight schedule | View track log | updated a few seconds ago

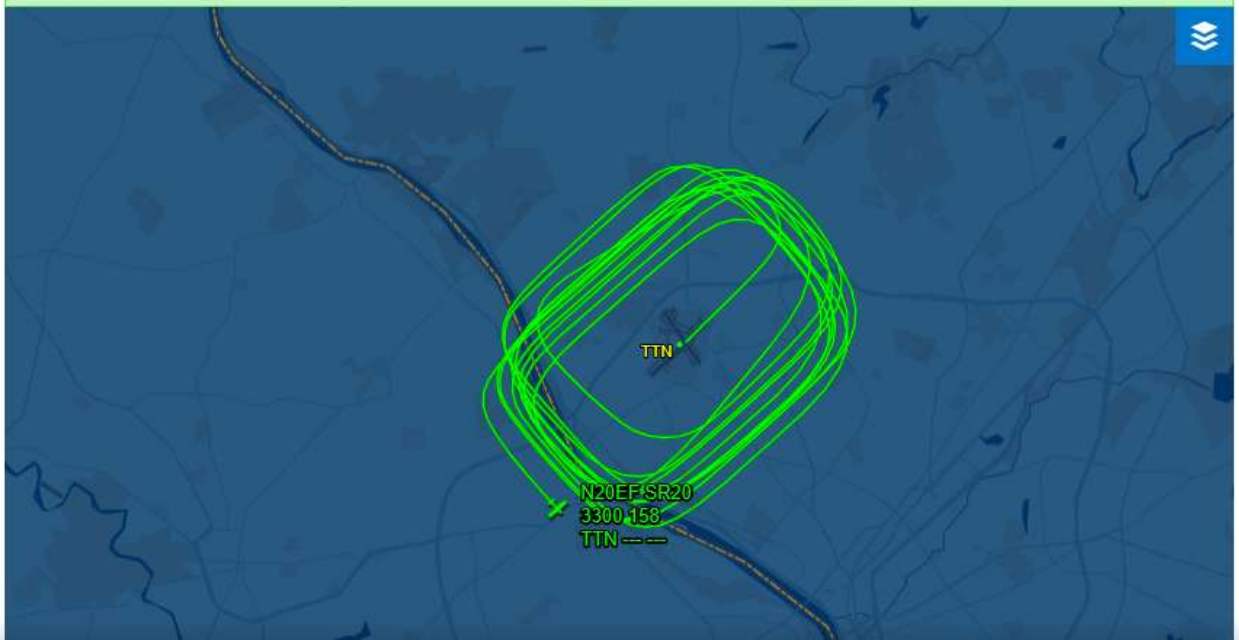
Set Up Unlimited Flight Alerts & More

Check out premium account features for aviation professionals and enthusiasts.

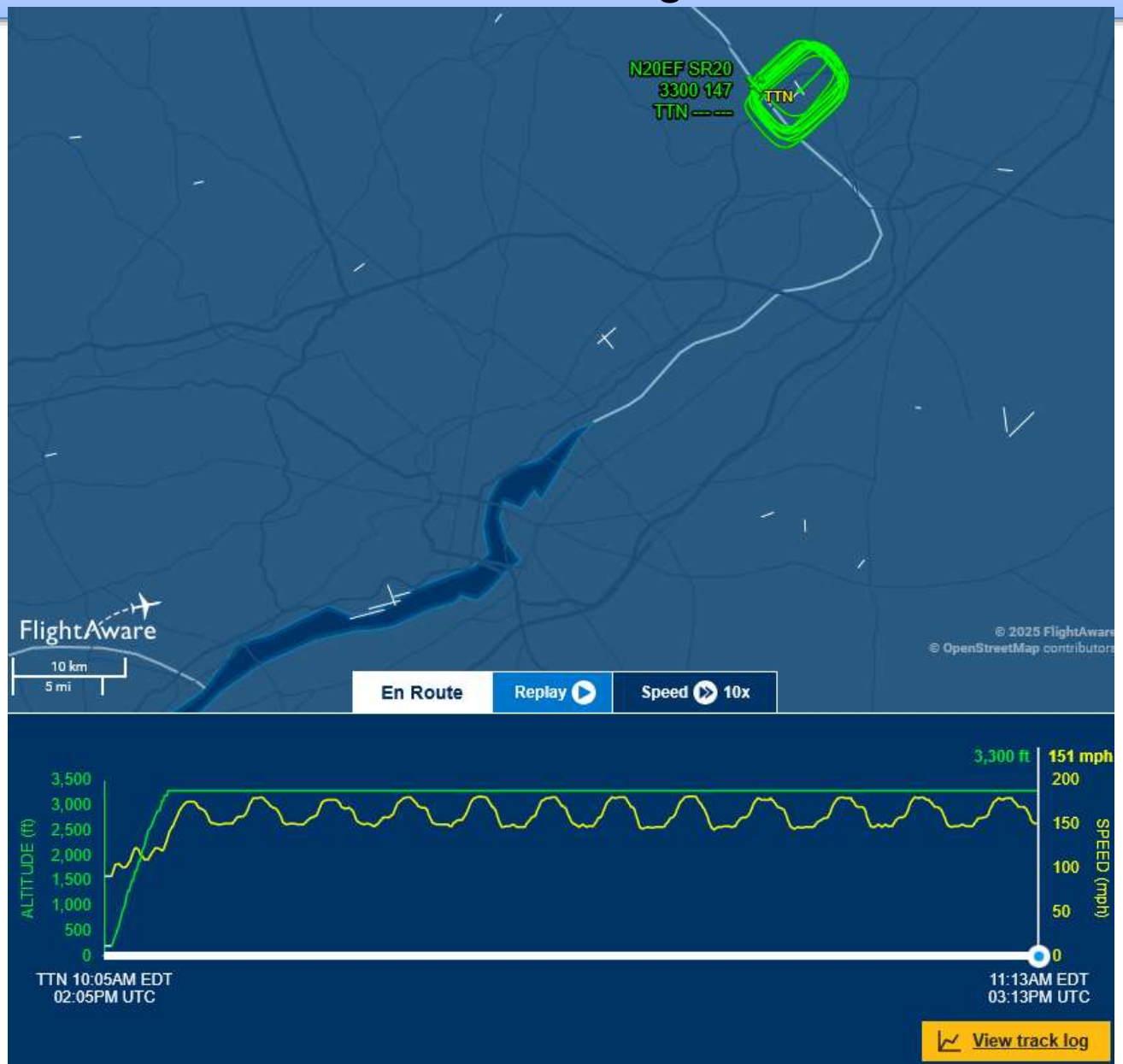
Discover FlightAware Premium

Show Features

Position-Only Flight | Learn More



Automatic Dependent Surveillance - Broadcast (ADS-B) is an advanced surveillance technology that combines an aircraft's positioning source, aircraft avionics, and a ground infrastructure



Automatic Dependent Surveillance - Broadcast (ADS-B) is an advanced surveillance technology that combines an aircraft's positioning source, aircraft avionics, and a ground infrastructure

FlightAware

All ▾ Search for flight, tail, airport, or city Forgot the flight number?

Products Industries ADS-B Flight Tracking

Return to Browse Photos | Upload Your Photos | Share This

2 Votes (5.00 Average) and 1,301 Views

Automatic Dependent Surveillance - Broadcast (ADS-B) is an advanced surveillance technology that combines an aircraft's positioning source, aircraft avionics, and a ground infrastructure

Registration/Tail #

N20EF

View Aircraft Registration

Live N20EF flight tracker
View N20EF flight history
View N20EF photos

Want more information about this aircraft? You might be interested in our FBO ToolBox service. Click here.

N20EF Aircraft Registration

Aircraft Summary

Summary	2021 CIRRUS DESIGN CORP SR20 Fixed wing single engine (4 seats / 1 engine)
Owner	EFENJ LLC PRINCETON , NJ, US
Airworthiness Class	Standard/Normal
Serial Number	2700
Engine	LYCOMING IO-390-C3B6 (Reciprocating) Horsepower: 215
Weight	Less than 12,500lbs
Speed	Not defined
Mode S Code	050310024 / A19014

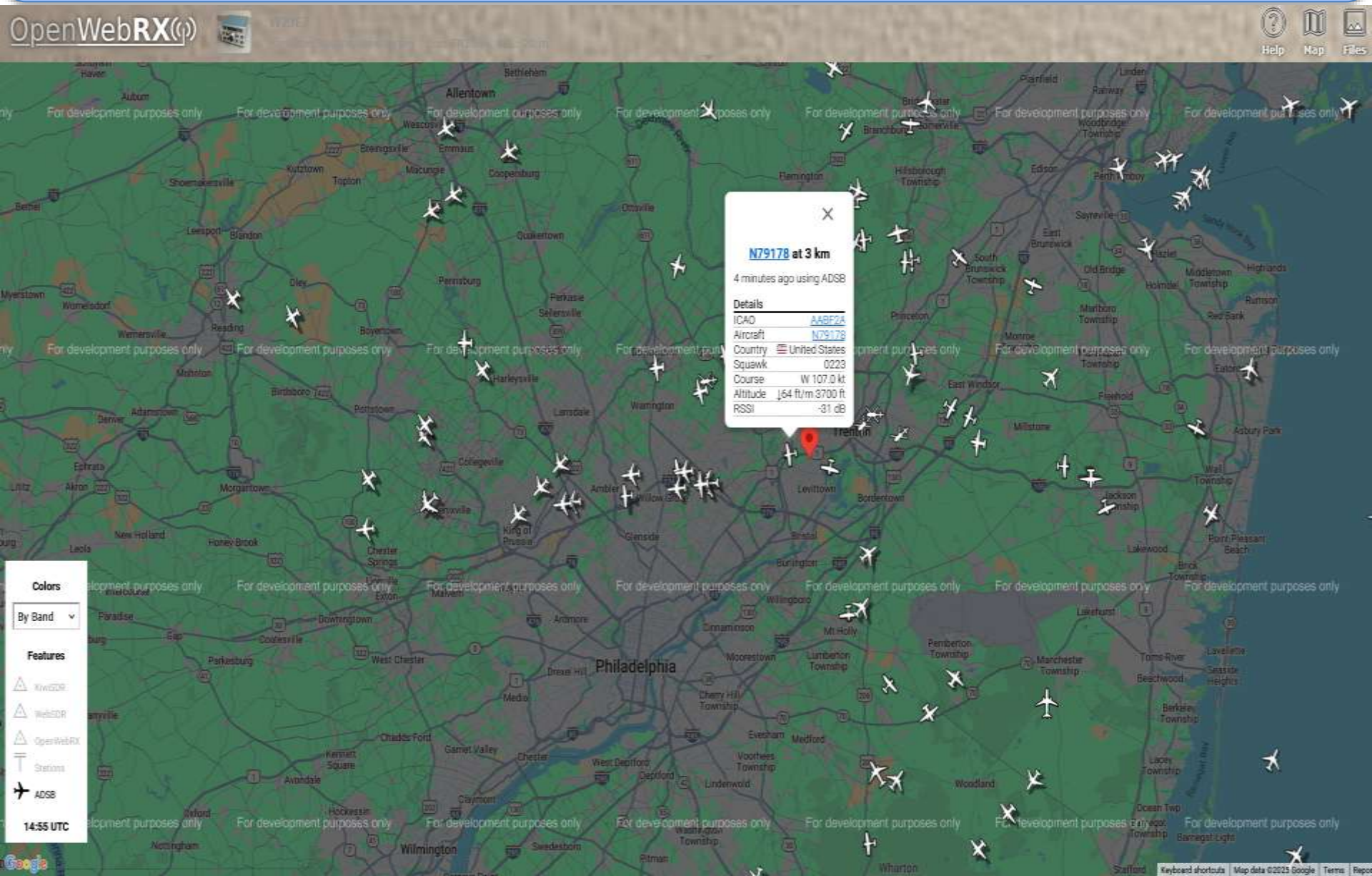
Registration Details

Status	Assigned
Certificate Issue Date	2021-07-01
Airworthiness Date	2021-04-05
Last Action Date	2023-04-19
Expiration	2028-07-31
Registry Source	FAA

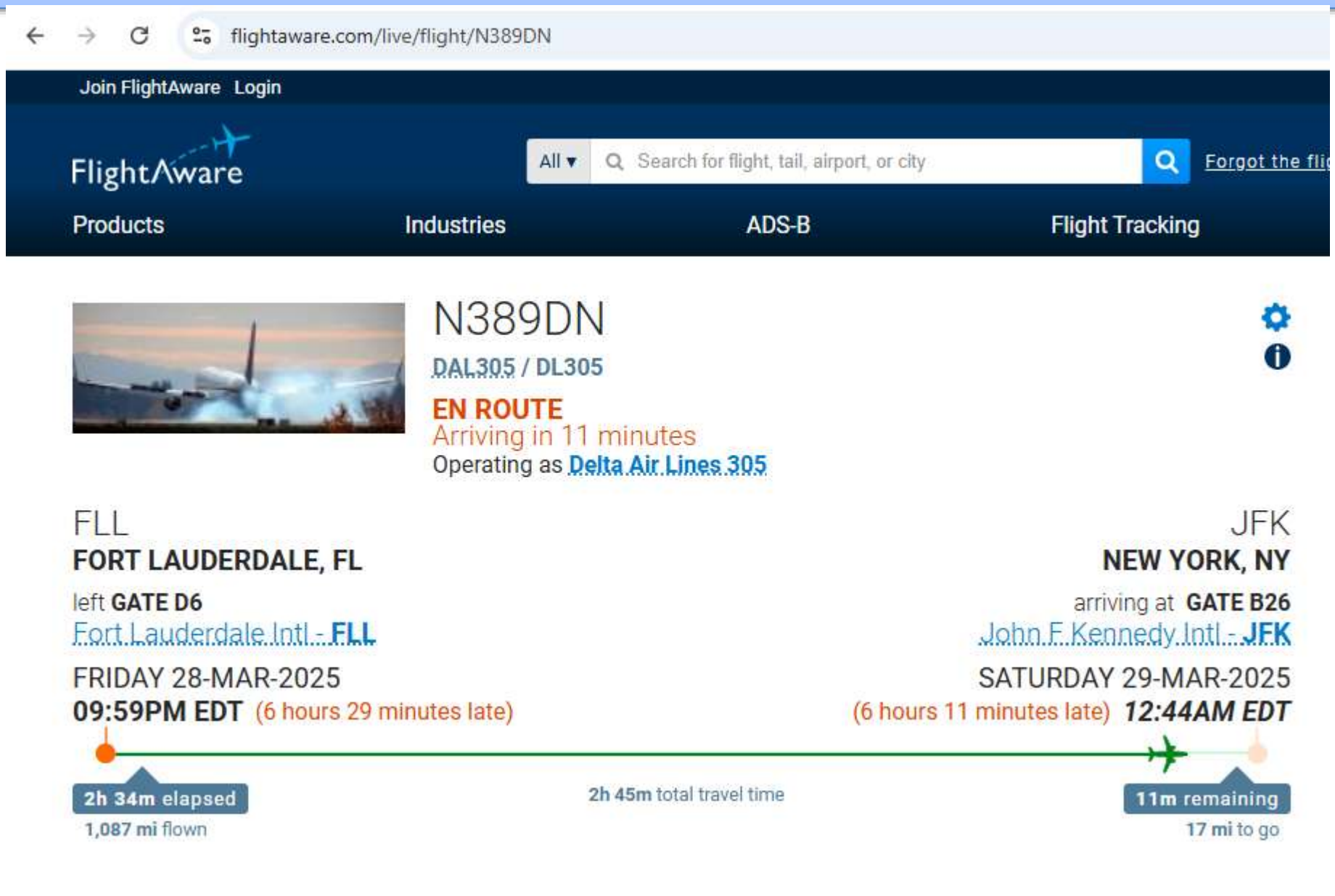
Registration History

Date	Owner	Location	Serial Number
01-Jul-2021	EFENJ LLC	PRINCETON NJ	2700
12-Feb-2021	CIRRUS DESIGN CORP	DULUTH MN	2700
14-Jul-2006	SALE REPORTED	EAST TROY WI	T26-157
02-Jun-2006	AIR CARGO CARRIERS INC	MILWAUKEE WI	T26-157

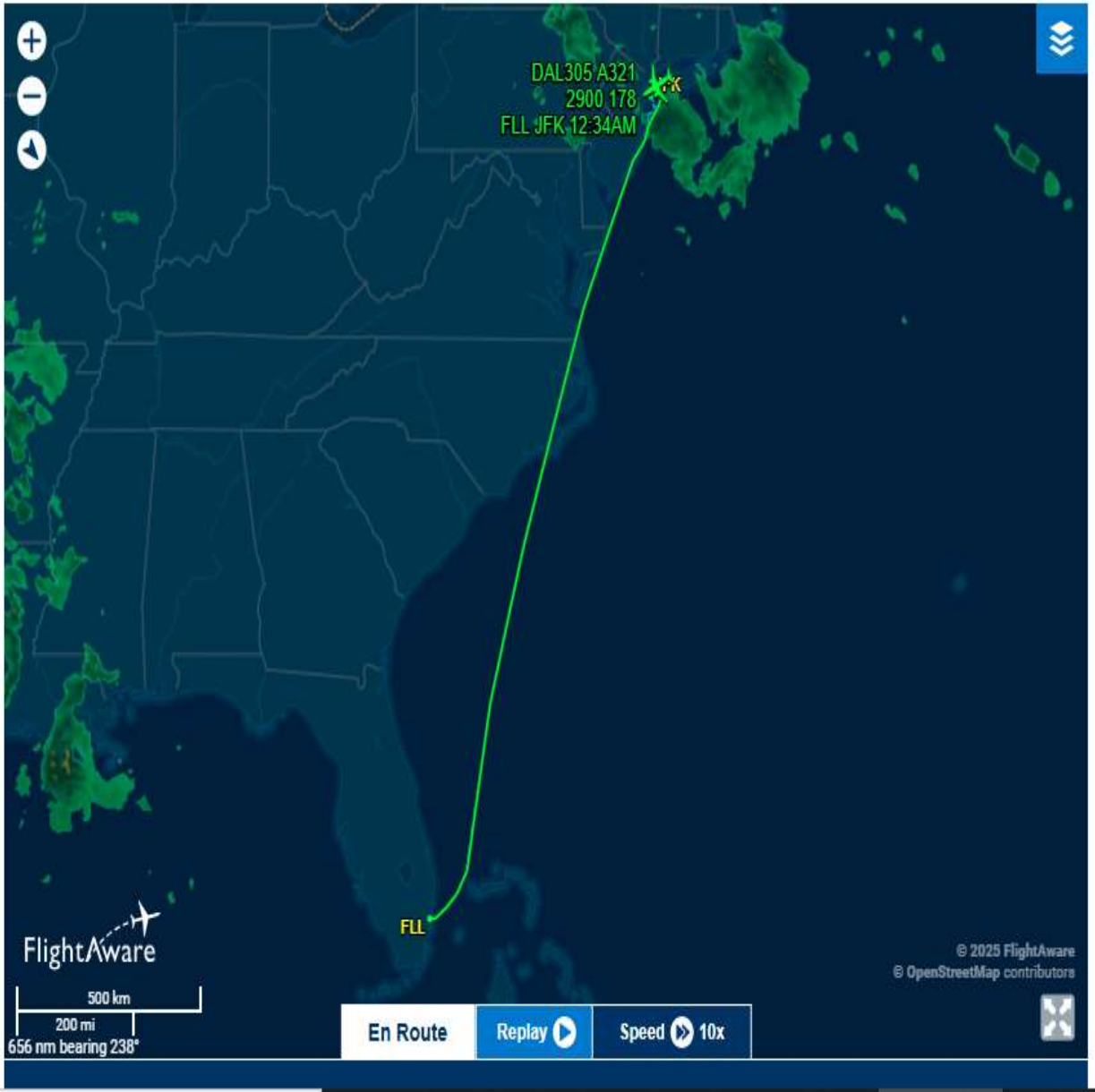
Automatic Dependent Surveillance - Broadcast (ADS-B) is an advanced surveillance technology that combines an aircraft's positioning source, aircraft avionics, and a ground infrastructure



Automatic Dependent Surveillance - Broadcast (ADS-B) is an advanced surveillance technology that combines an aircraft's positioning source, aircraft avionics, and a ground infrastructure



Automatic Dependent Surveillance - Broadcast (ADS-B) is an advanced surveillance technology that combines an aircraft's positioning source, aircraft avionics, and a ground infrastructure



Get Alerts

Flight Details

updated a few seconds ago

View track log

Track inbound plane

All flights between FLL and JFK

Departure Times

Gate Departure	Takeoff
09:59PM EDT	**10:15PM EDT**
Scheduled 03:30PM EDT	Scheduled 03:40PM EDT

Taxi Time: 16 minutes

Average Delay: Less than 10 minutes

Arrival Times

Landing	Gate Arrival
12:34AM EDT (+1)	***12:44AM EDT (+1)***
Scheduled 06:01PM EDT	Scheduled 06:33PM EDT

Taxi Time: *10 minutes*

Average Delay: Less than 10 minutes

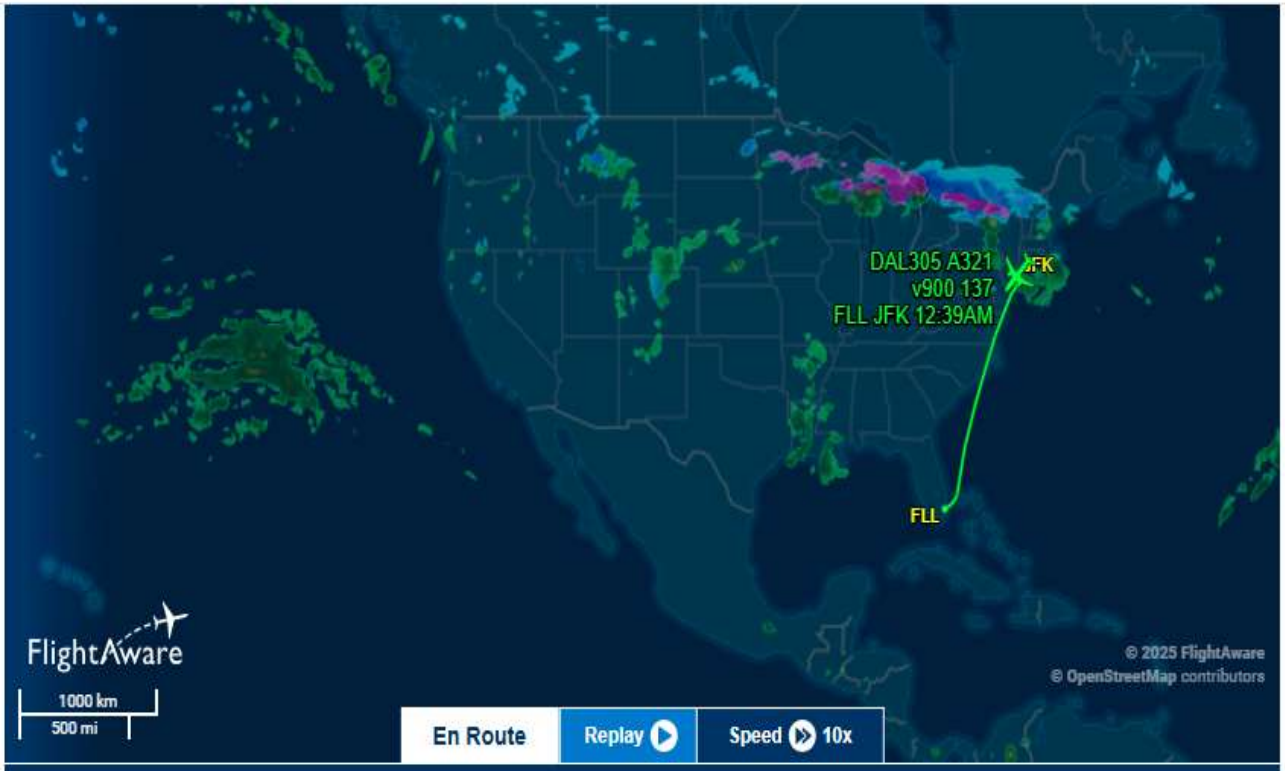
Aircraft Details

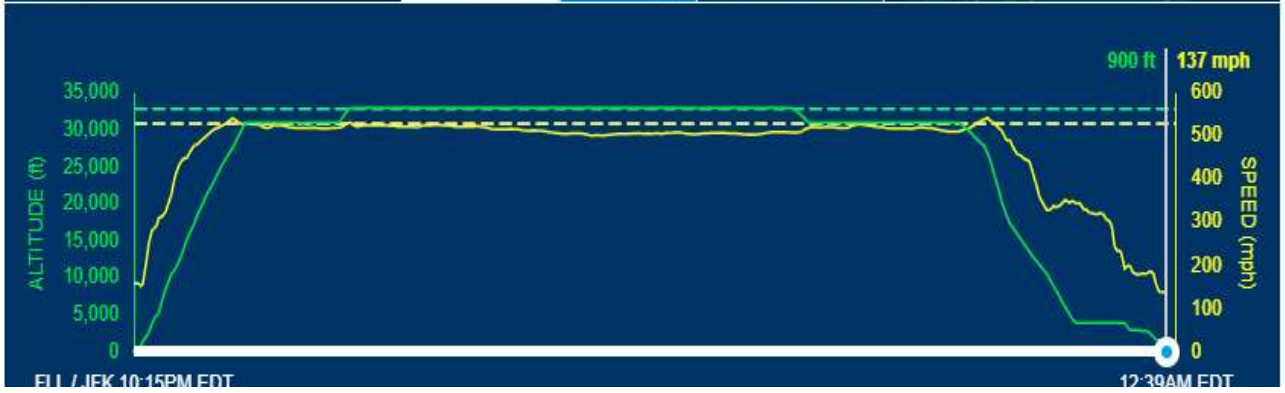
updated a few seconds ago

Aircraft Information

Automatic Dependent Surveillance - Broadcast (ADS-B) is an advanced surveillance technology that combines an aircraft's positioning source, aircraft avionics, and a ground infrastructure

flightaware.com/live/flight/N389DN





Gate Departure	Takeoff
09:59PM EDT	**10:15PM EDT**
Scheduled 03:30PM EDT	Scheduled 03:40PM EDT

Taxi Time: 16 minutes

Average Delay: Less than 10 minutes

Arrival Times

Landing	Gate Arrival
12:39AM EDT (+1)	***12:44AM EDT (+1)***
Scheduled 06:01PM EDT	Scheduled 06:33PM EDT

Taxi Time: *5 minutes*

Average Delay: Less than 10 minutes

Aircraft Details

updated a few seconds ago

Aircraft Information

Tail Number	N389DN · Registration
Owner	BANK OF UTAH TRUSTEE
Aircraft Type	Airbus A321 (twin-jet) (A321)

Photos

Airline Information

Airline	Delta Air Lines "Delta"

all flights

Flight Data

SIGNALS INTELLIGENCE – RF SIGNATURE

sigidwiki.com/wiki/Signal_Identification_Guide

- Amateur Radio
- Trunked Radio
- Numbers Stations
- Commercial
- Utility
- Time

tools

- What links here
- Related changes
- Special pages
- Printable version
- Permanent link
- Page information
- Browse properties

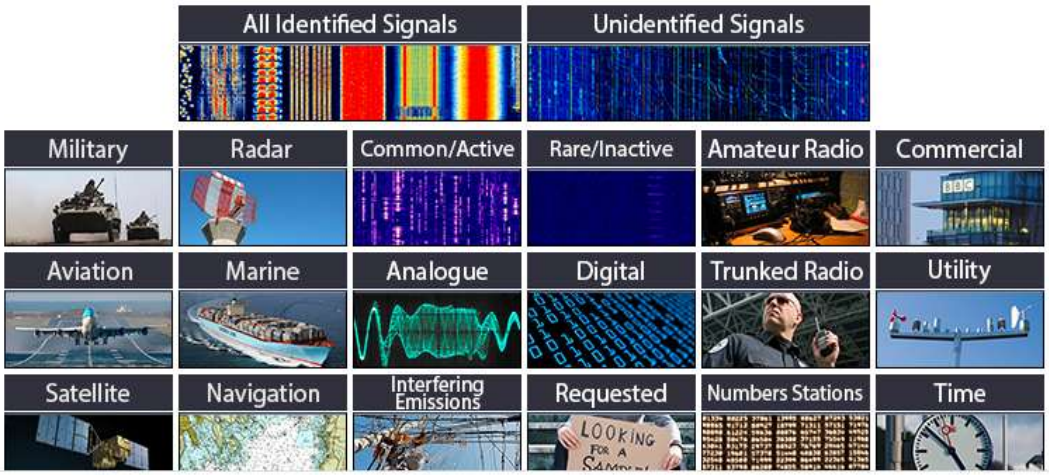
Ads by Google

Stop seeing this ad

Why this ad?

Frequency Bands

Categories



Coverage compari....pdf | Coverage Analysis....pdf | On the Coverage o....pdf | Measurementofele....pdf | RF bugs-GS days 2....pdf | Show all

RF and modulation signal patterns

https://www.sigidwiki.com/wiki/Signal_Identification_Guide

TEKTRONICS SOLUTION
Detecting Drones Using a Real-Time Spectrum Analyzer

Nearly all drones:

- Are controlled locally within a visual range of about 1000 ft.
- Are controlled remotely within 2-3 miles using First Person View (FPV)
- Operate in the 2.4 GHz unlicensed band for control (approx. 80 MHz bandwidth)
- Use 5.8 GHz unlicensed band for first person view (FPV) video feeds (20 MHz or less)
- Employ return to home (RTH) when control signals are lost or weak
- Utilize drone control signals that normally hop across multiple frequencies and can be up to 80 MHz wide
- The FCC has designated that drones can only be operated in the unlicensed bands, including the 2.4 GHz, 5.8 GHz, 900 MHz and 433 MHz bands

https://download.tek.com/document/Detecting%20Drones%20Using%20a%20RTSA%20App-Note%2037W615760.pdf?

TEKTRONICS SOLUTION
Detecting Drones Using a Real-Time Spectrum Analyzer

Basic Drone Detection

Basic drone detection can be performed with a Tektronix RSA306B or RSA500 Series Spectrum Analyzer and Tektronix DataVu-PC software. As drone operators generally use a first-person video (FPV) link to track of the drone's location, the first step in looking for a drone's presence is to scan the 5.8 GHz band to look for burst signals that are present as the drone and controller communicate to each other.
As mentioned above, hobbyist and commercial drones transmit video in the 5.8 GHz unlicensed band. Transmitting video or control signals from th drone to the pilot results in recognizable bursts of RF energy that occur as the transmitter and receiver acknowledge receipt of data.

The Tektronix RSA306B and RSA500.

https://download.tek.com/document/Detecting%20Drones%20Using%20a%20RTSA%20App-Note%2037W615760.pdf?

TEKTRONICS SOLUTION
Detecting Drones Using a Real-Time Spectrum Analyzer

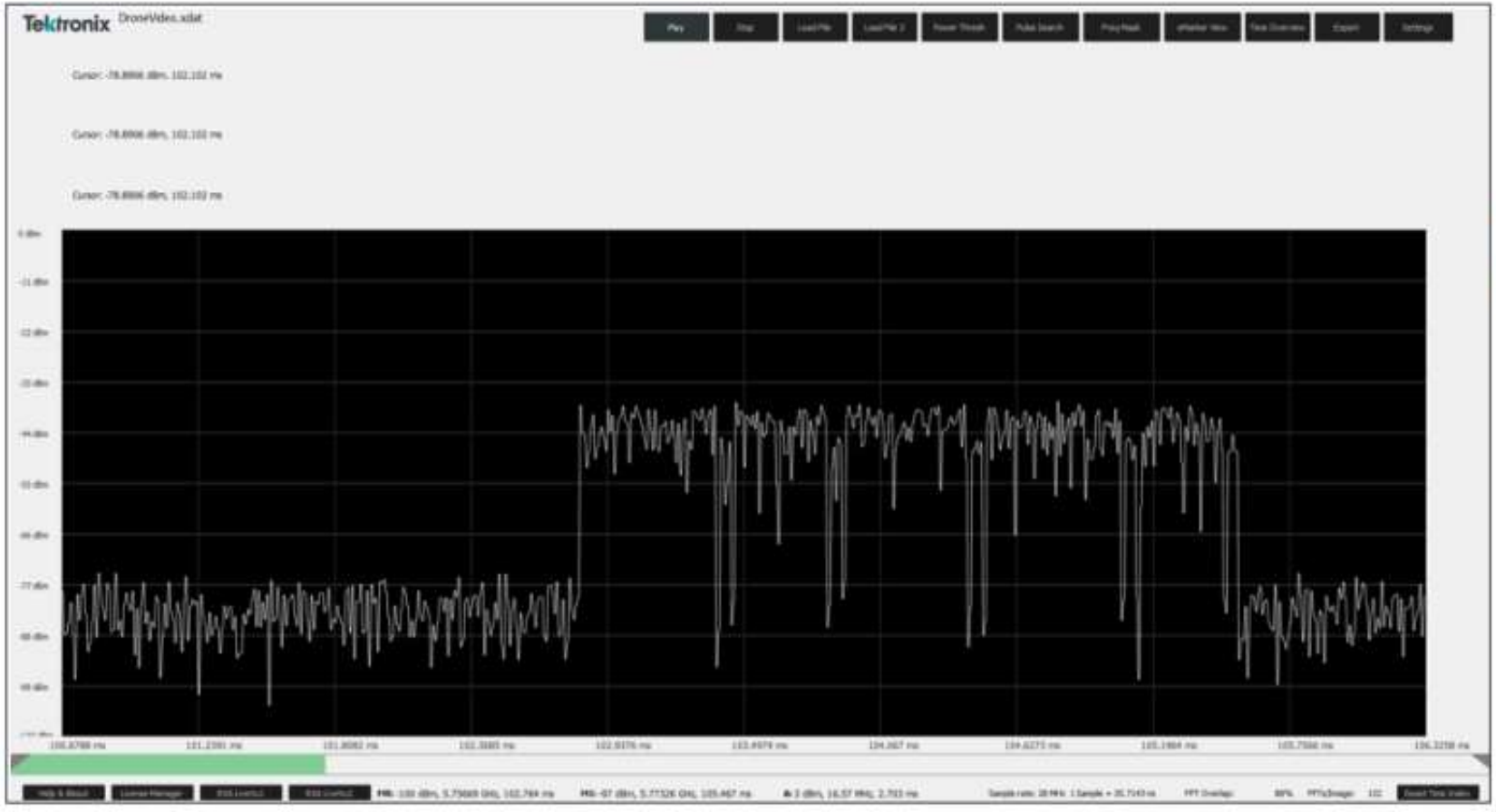


FIGURE 1. Video burst from 5.8 GHz frequency band.

https://download.tek.com/document/Detecting%20Drones%20Using%20a%20RTSA%20App-Note%2037W615760.pdf?

TEKTRONICS SOLUTION
Detecting Drones Using a Real-Time Spectrum Analyzer

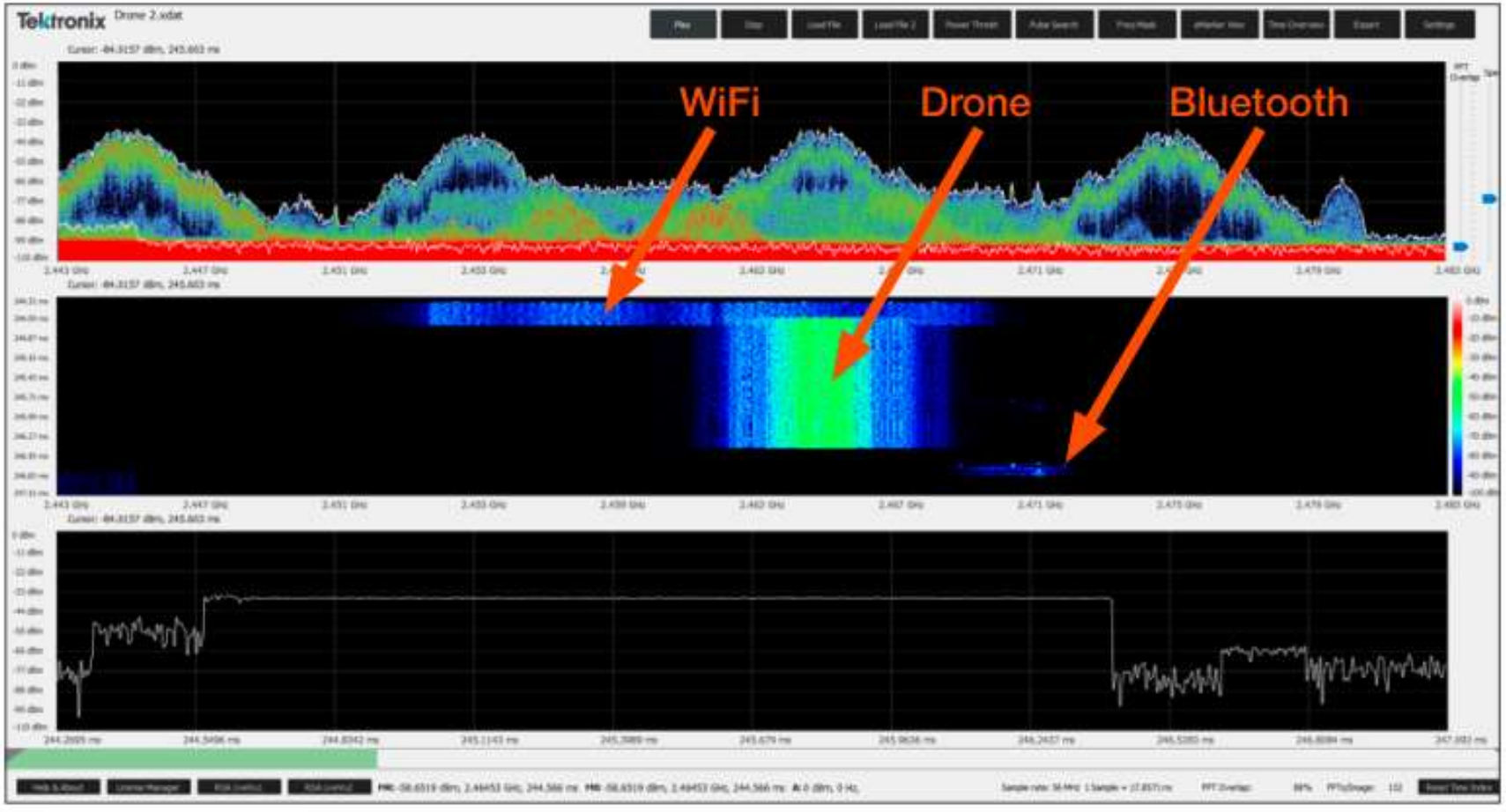


FIGURE 2. Control bursts from 2.4 GHz frequency band.

https://download.tek.com/document/Detecting%20Drones%20Using%20a%20RTSA%20App-Note%2037W615760.pdf?

TEKTRONICS SOLUTION
Detecting Drones Using a Real-Time Spectrum Analyzer

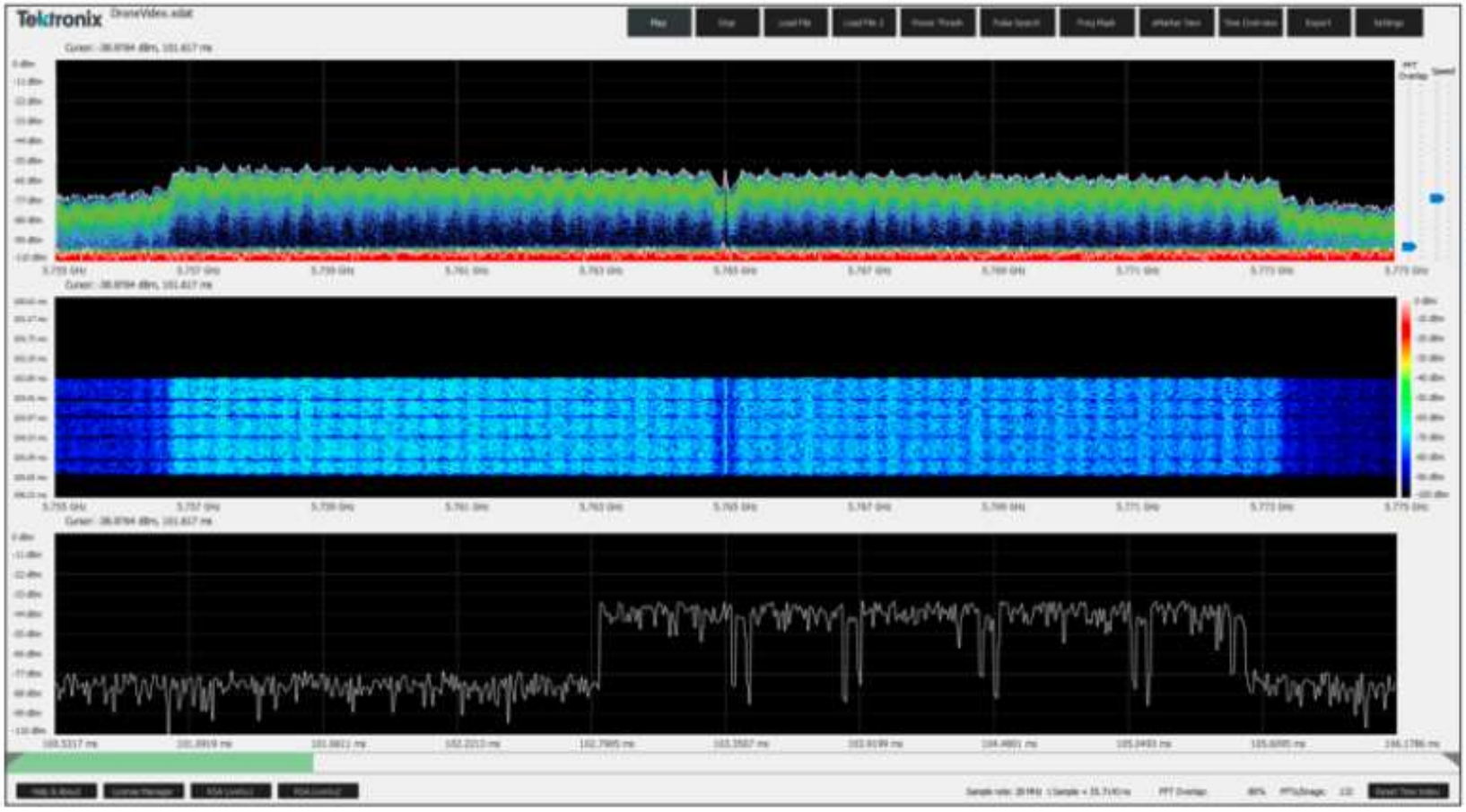


FIGURE 3.
Video burst from 5.8 GHz frequency band using I/Q processing.

https://download.tek.com/document/Detecting%20Drones%20Using%20a%20RTSA%20App-Note%2037W615760.pdf?

TEKTRONICS SOLUTION
Detecting Drones Using a Real-Time Spectrum Analyzer

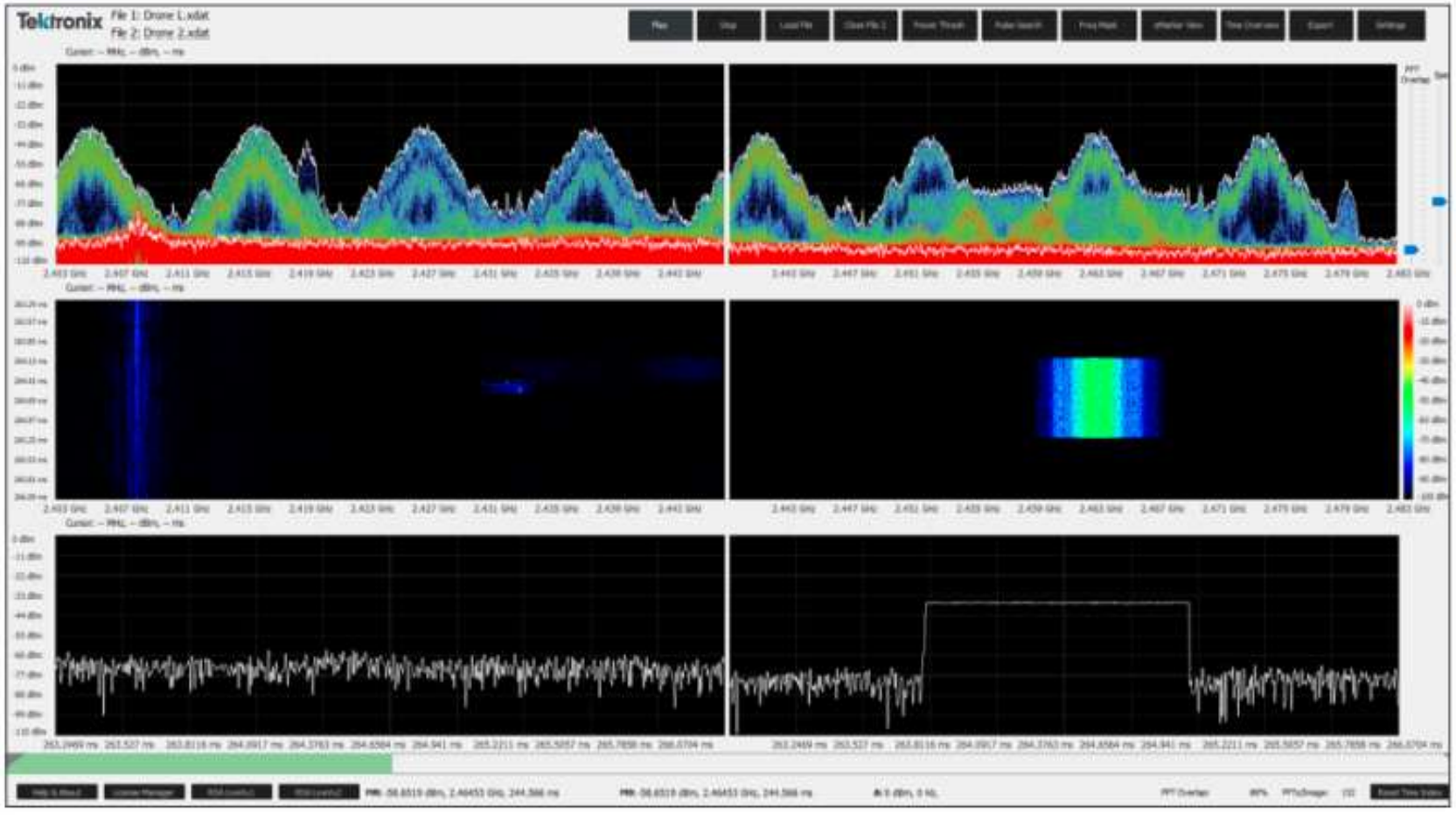
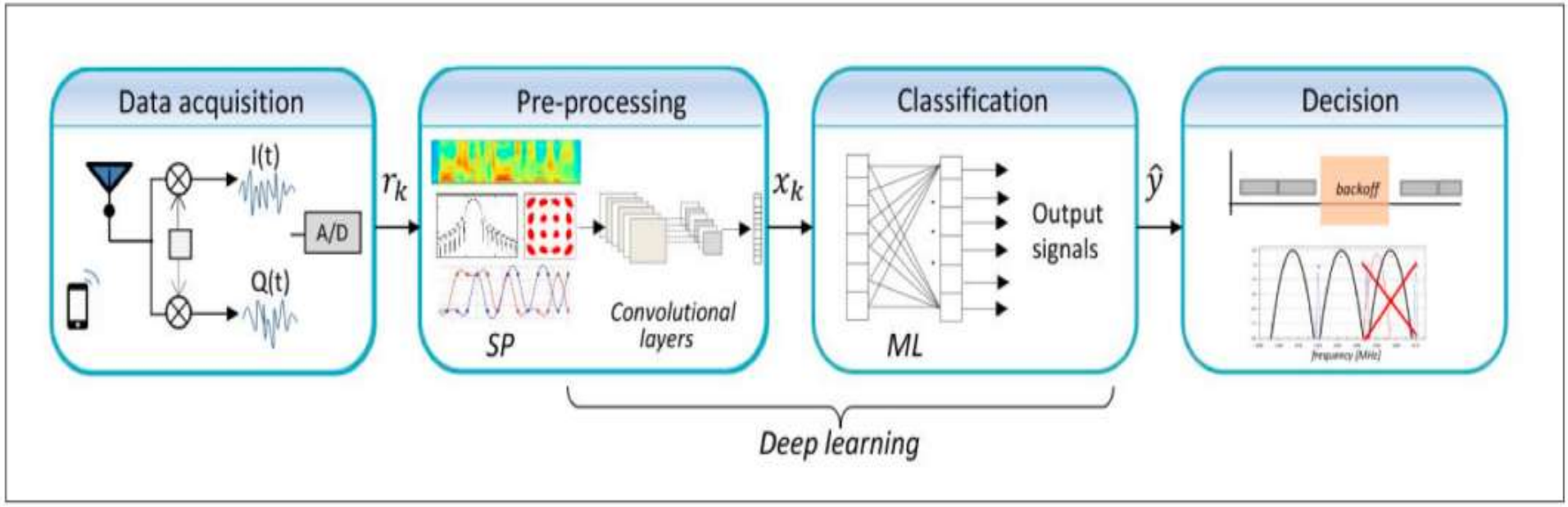


FIGURE 4. Dual RSA mode showing the hopping frequencies and sequences of the drone controller.

https://download.tek.com/document/Detecting%20Drones%20Using%20a%20RTSA%20App-Note%2037W615760.pdf?

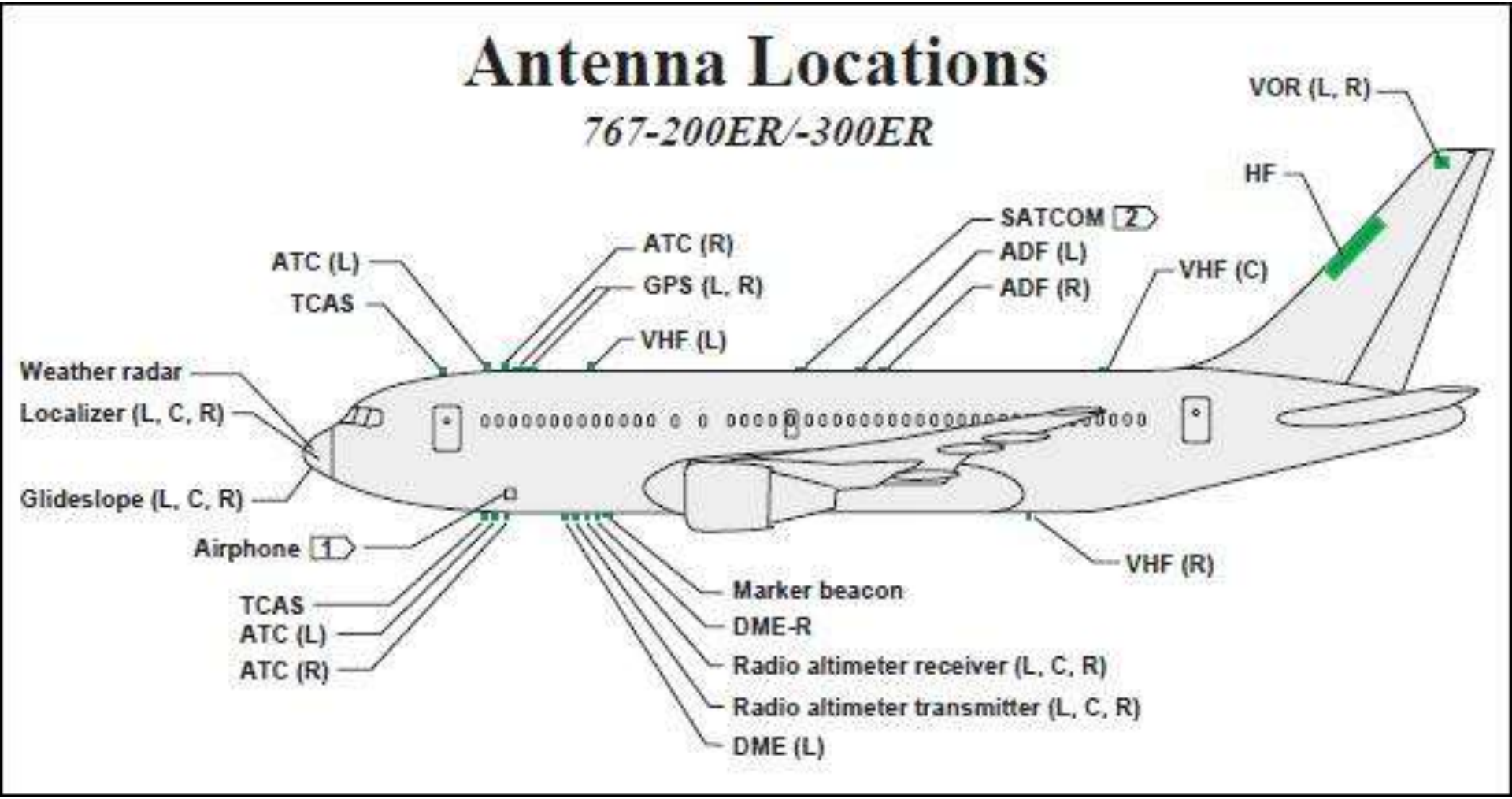
TEKTRONICS SOLUTION
Detecting Drones Using a Real-Time Spectrum Analyzer



Processing pipeline for end-to-end learning from spectrum data.[2]

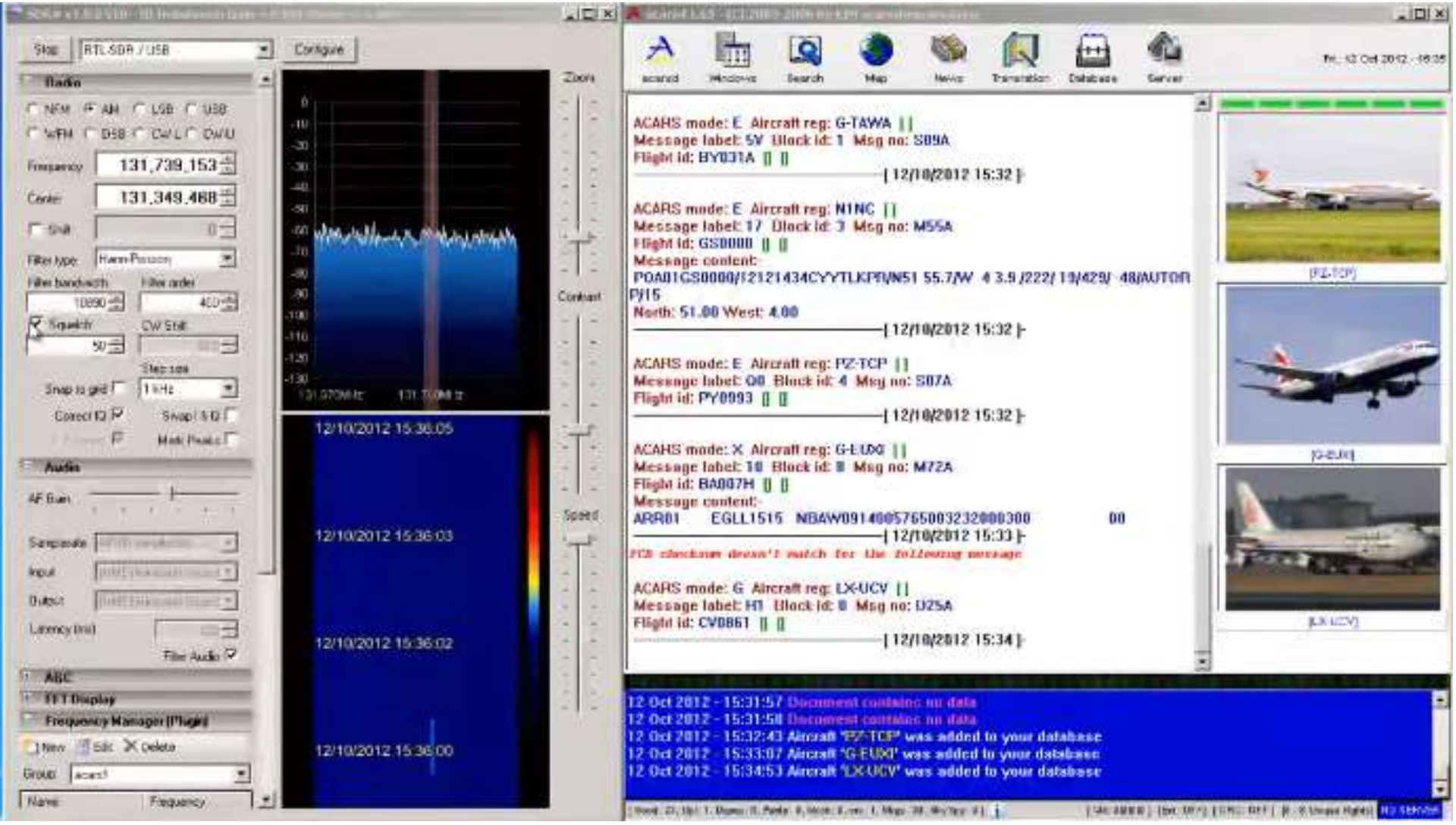
https://download.tek.com/document/Detecting%20Drones%20Using%20a%20RTSA%20App-Note%2037W615760.pdf?

RTL-SDR AIRCRAFT MONITORING



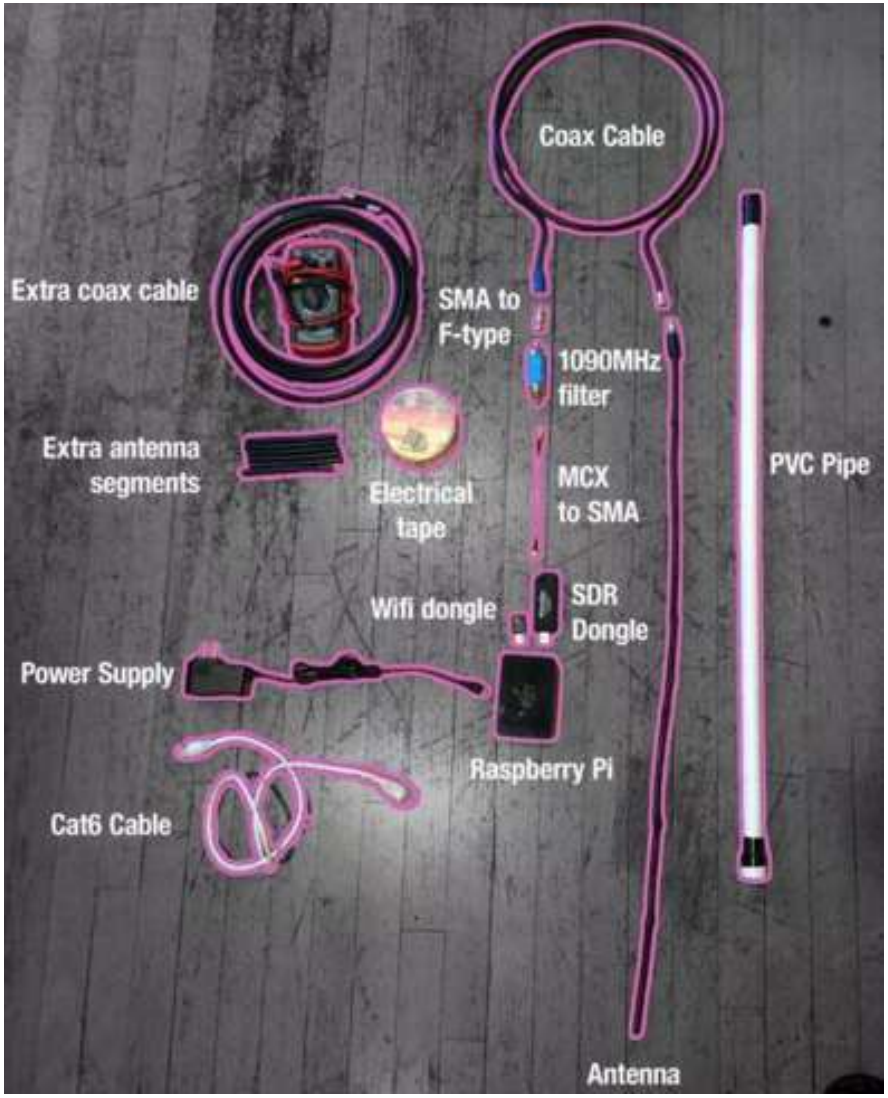
AIRCRAFT ACARS

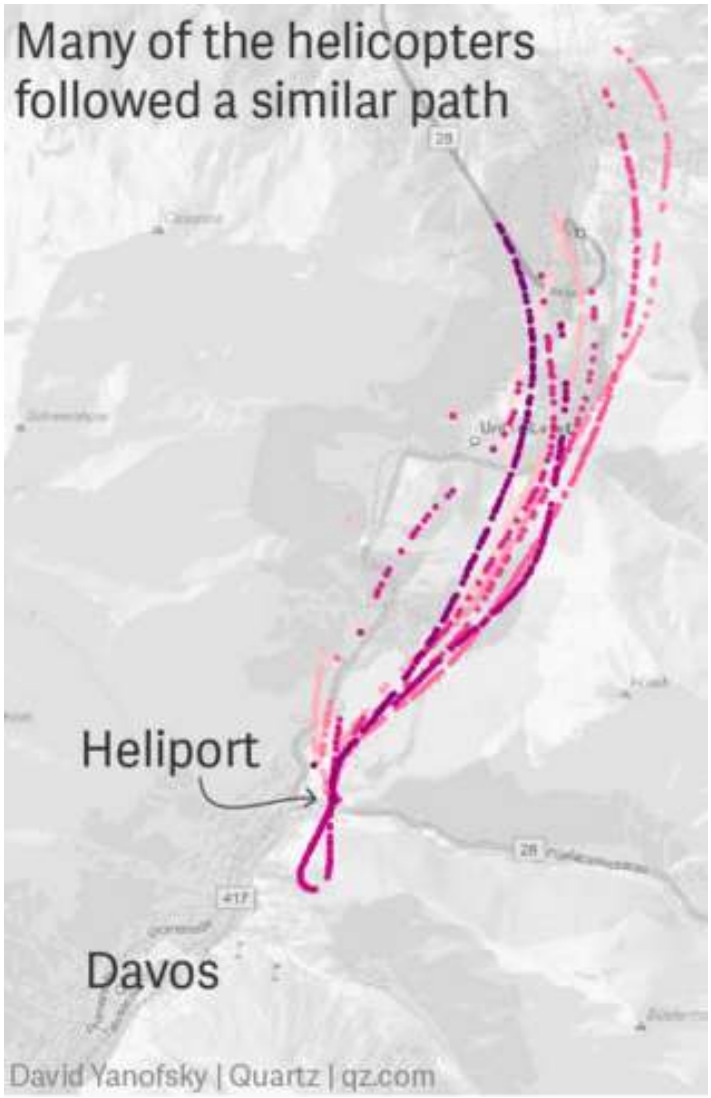
AIRCRAFT ACARS IS VHF, HF, AND SATELLITE



ADS-B AIRCRAFT AND HELICOPTER

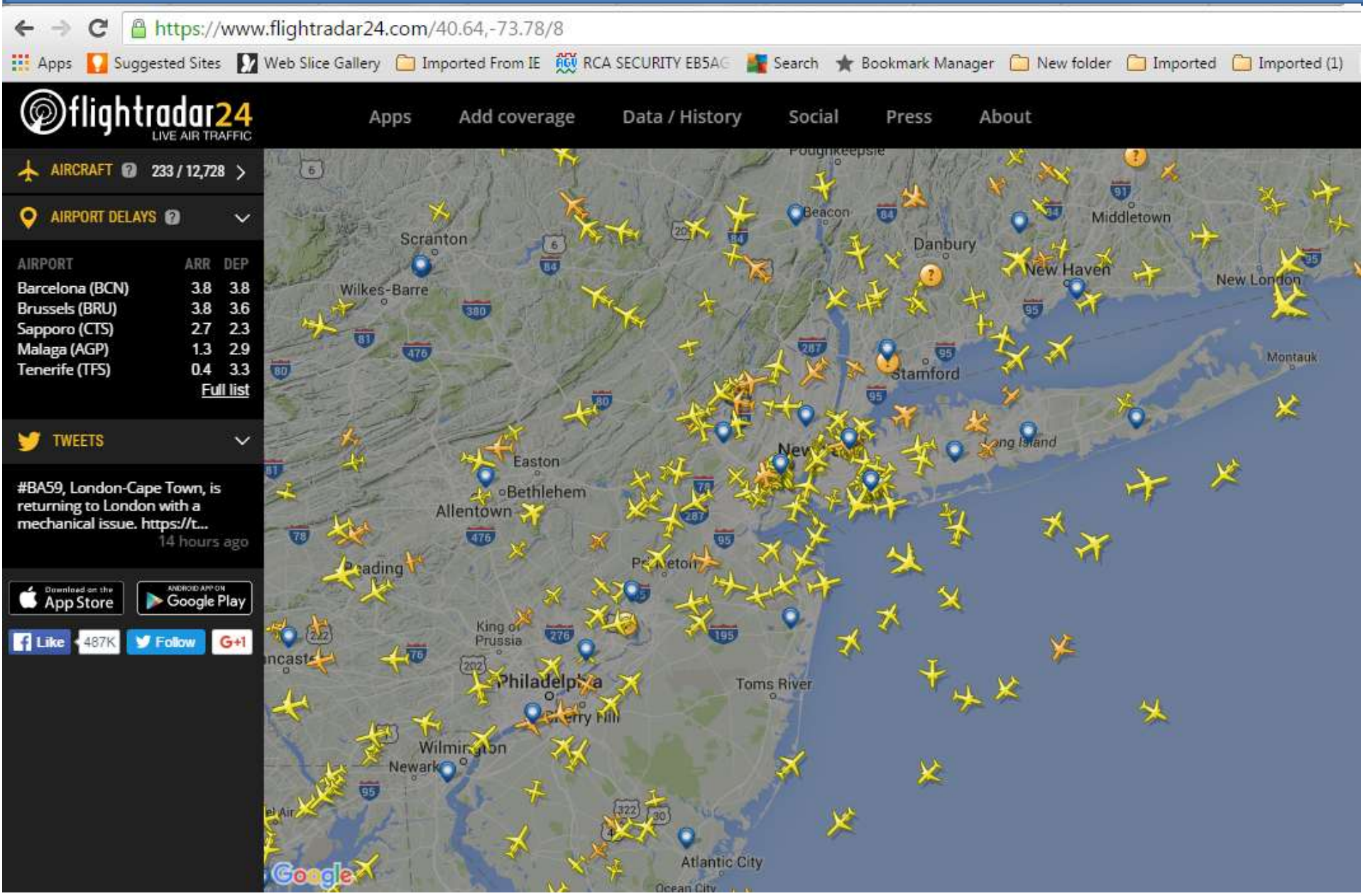
TRACKING THE WORLD ECONOMIC HEADQUARTERS' TRANSPORATION HELICOPTERS @ 1090 MHz (Automatic Dependent Surveillance Location Tracking System)





http://qz.com/600590/we-brought-an-antenna-to-davos-to-track-private-air-travel-and-heres-what-we-

UPLOADED AND SHARED ADS-B



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

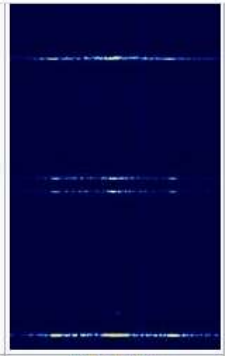
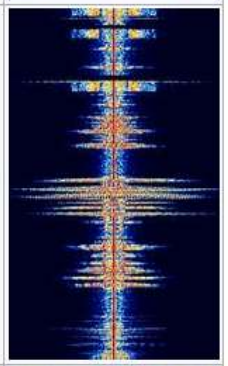
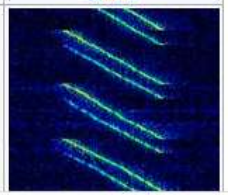
EMERGENCY COMMUNICATIONS – HURRICANE MARIA STRUCK DOMINICA @ 175 mph, CAT 5

11/06/2017
AT&T is using an LTE cell payload UAV to offer connectivity to Puerto Ricans who lost wireless service after Hurricane Maria and live in a 40-mile (max) area under the UAV CELL ON WINGS.

This photo was taken over a month after hurricane Maria devastated Puerto Rico where 48 percent of cell sites remain inoperative.

SIGNALS INTELLIGENCE – RF SIGNATURE

sigidwiki.com/wiki/Category:Marine

Automatic Identification System (AIS)	Automatic Identification System (AIS) is used by ships to broadcast position and vessel information.	161.975 MHz — 162.025 MHz	NFM	GMSK	25 kHz	Worldwide	0:05 / 0:14	
Automatic Transmitter Identification System (ATIS)	ATIS systems are identification tags used by inland commercial waterway traffic on rivers in Europe. The FSK burst is appended at the end of every voice transmission by the vessel operator.	30 MHz — 800 MHz	NFM	FSK	12 kHz	Europe	0:00 / 0:00	
CODAR	CODAR (Coastal Ocean Dynamics Applications Radar) is used for near-surface	4.438 MHz —	USB	ILFM	50 kHz	Worldwide	0:00 / 0:00	

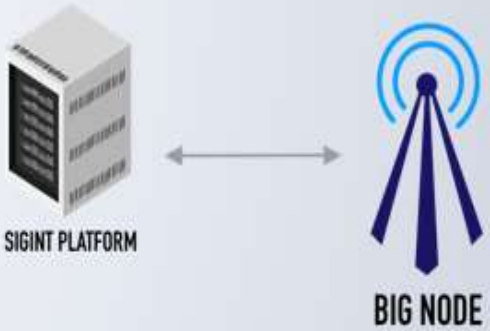
Coverage compari....pdf | Coverage Analysis....pdf | On the Coverage o....pdf | Measurementofele....pdf | RF bugs-GS days 2....pdf | Show all

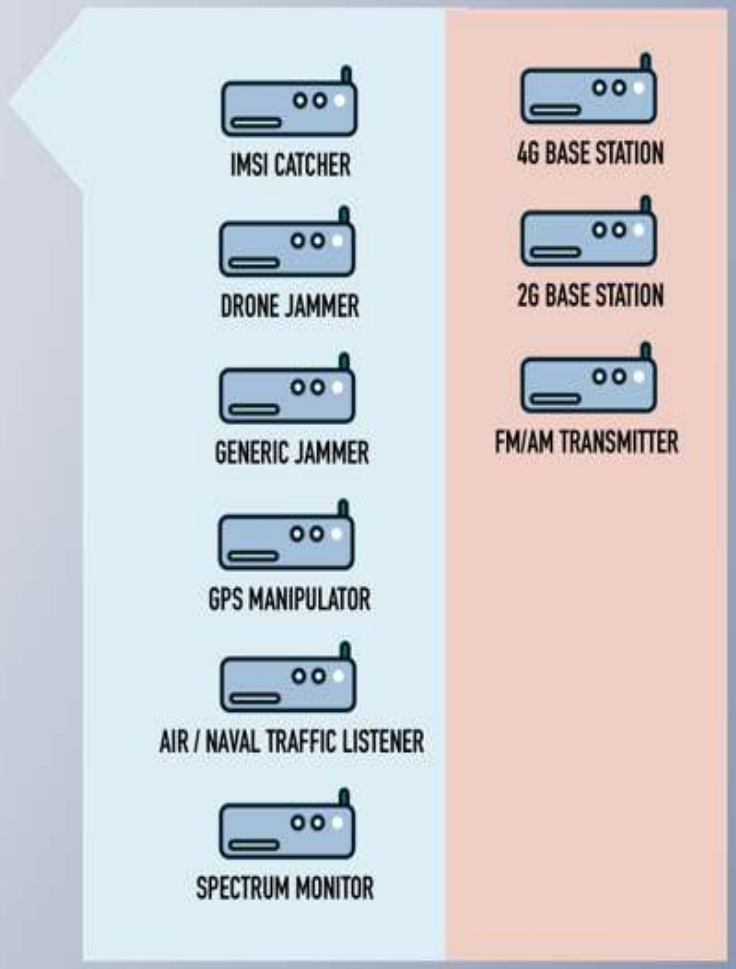
Marine RF and modulation signal patterns

https://www.sigidwiki.com/wiki/Category:Marine

CELLULAR DATA SECURITY - SigintOS

NODES





BIG NODE

MINI NODE; It is easily portable. It performs operations according to many different hardware and radio receivers in its content. These operations can be added or removed as modules.
In addition, FM and AM broadcasts can be made and 4G and 2G networks can be created completely privately.

SigintOS™

SIGINT PLATFORM

https://medium.com/@tomac/sigintos-a-wireless-pentest-distro-review-a7ea93ee8f8b

CELLULAR DATA SECURITY – SigintOS SDR, T-IMSI

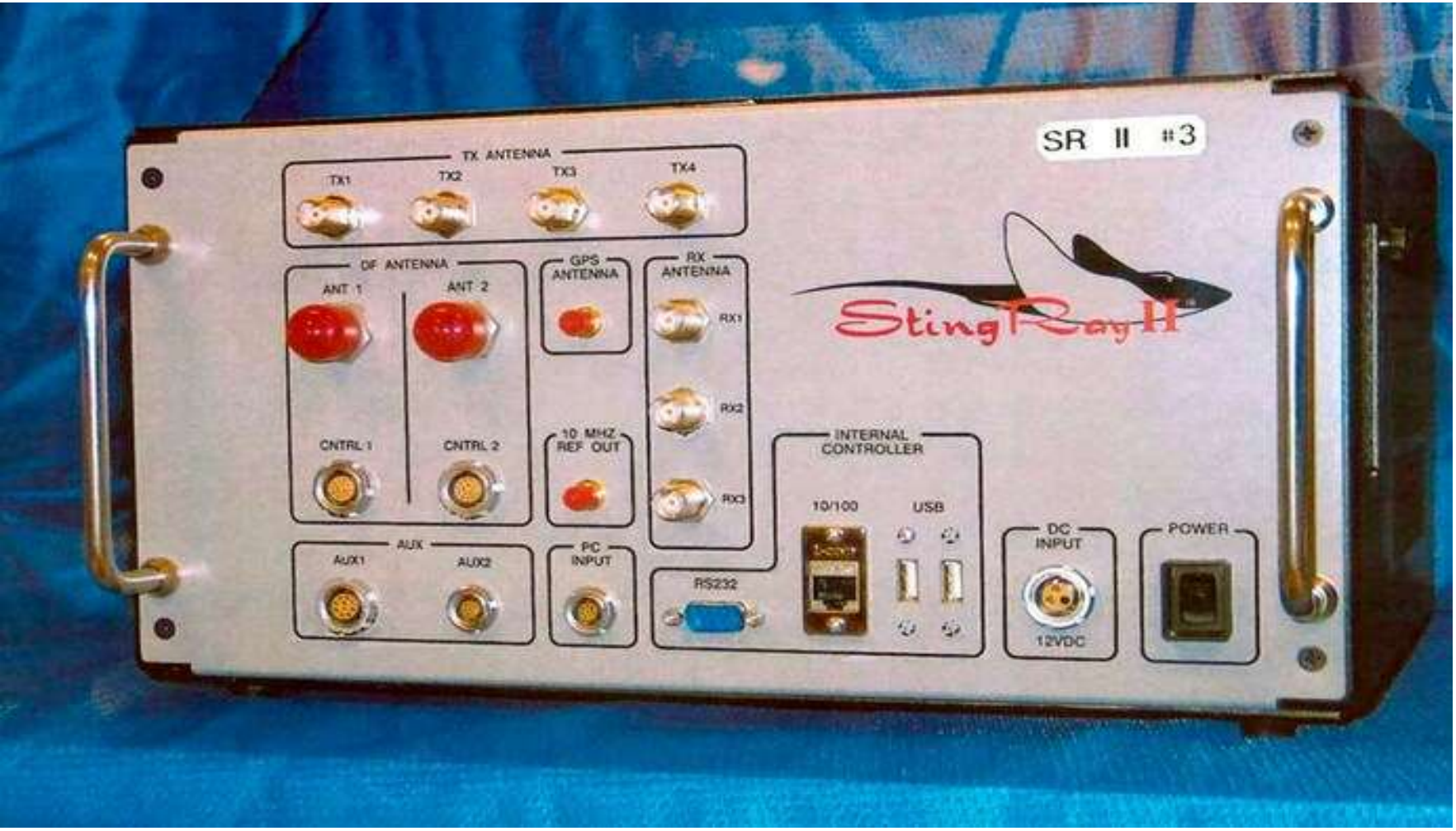
IMSI stands for International Mobile Subscriber Identity and is the identifier for the SIM card to which your mobile phone number is Linked.

TIMSI is the LTE 4G/5G Temporary International Mobile Subscriber Identity.

https://i-hls.com/archives/80949

https://medium.com/@tomac/sigintos-a-wireless-pentest-distro-review-a7ea93ee8f8b

CELLULAR DATA SECURITY, Historic StingRAY



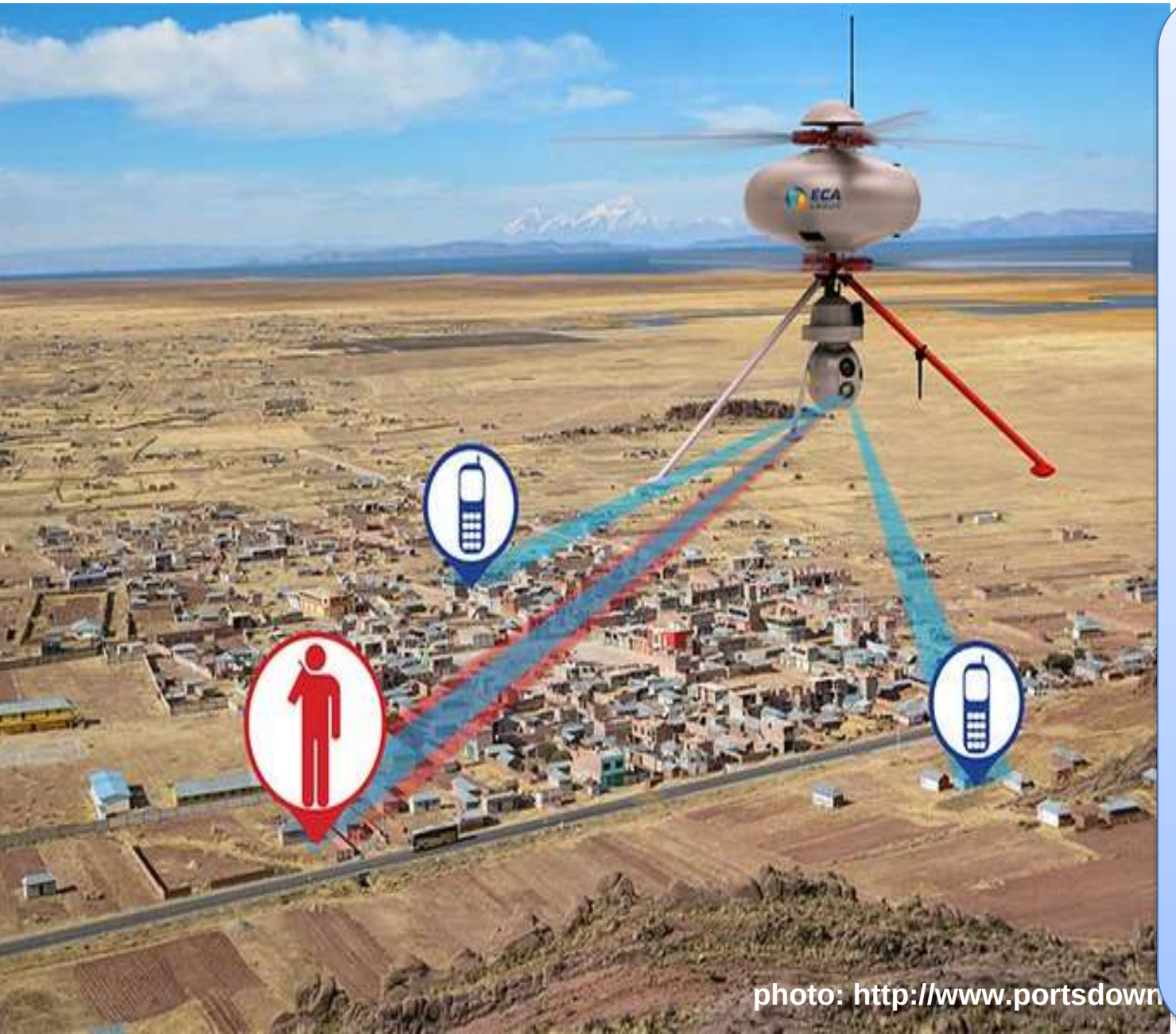
Fake Cell Site, the L3Harris StingRAY

https://www.washingtonpost.com/world/national-security/dhs-says-it-has-detected-possible-cellphone-surveillance-in-dc--and-doesnt-know-whos-doing-it/

CELLULAR DATA SECURITY

The Israeli companies unveiled their joint intelligence-gathering UAV at the Eurosatory exhibition in Paris. In the context of this cooperative effort, the Orbiter-3 UAV by Aeronautics carries the SigInt systems by Verint. Amir Rapaport reports from Paris https://israeldefense.co.il/en/node/34581

CELLULAR DATA SECURITY



The At MILIPOL 2017, ECA Group, unveiled the IMSI-Catcher signal intelligence module for its UAV IT180 mini-drone. A tool in the fight against terrorism.

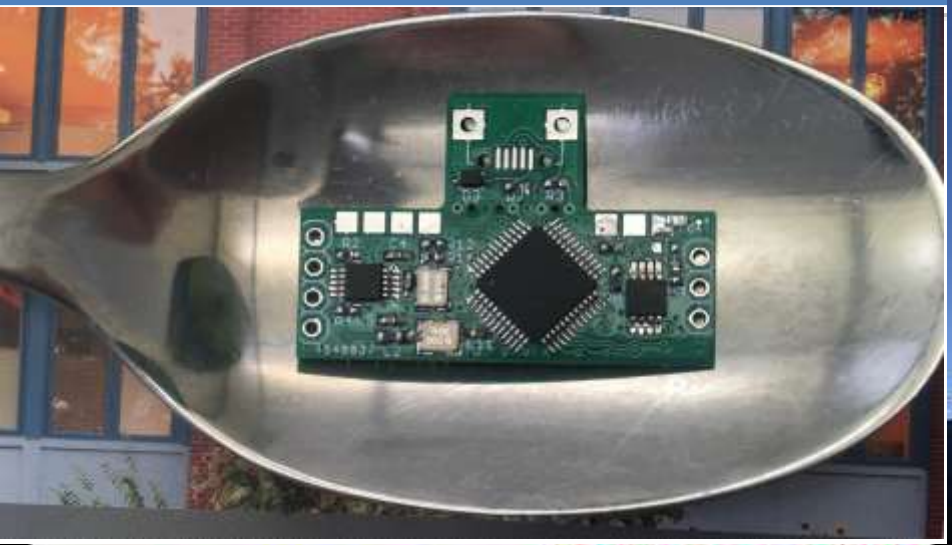
https://www.armyrecognition.com/milipol_paris_2017_news_online_show_daily/milipol_2017_eca_group_uav_it180_gets_new_sigint_payload.html

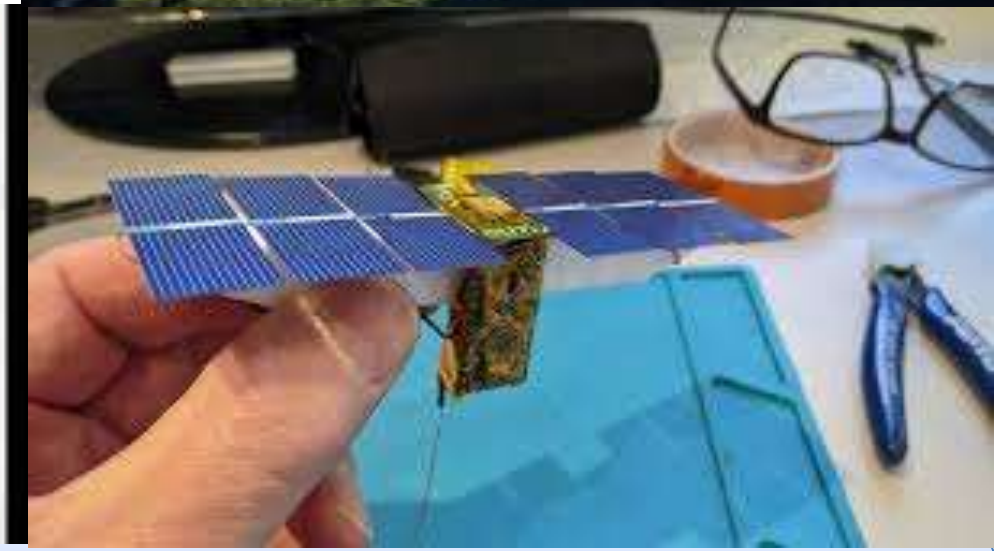
CHINESE PLA BALLOON HAP SECURITY

A US defense official said the balloon is the size of several buses - but doesn't post an immediate threat to Americans.

https://www.dailymail.co.uk/news/article-11712125/Explosion-sky-Billings-Montana-Chinese-balloon-spotted-U-S-airspace.html

GLOBAL EXPERIMENTAL BALLOON (HAP) SECURITY





Weighs only 1.8g and measurer just 33.0 x 12.7mm!

https://qrp-labs.com/u4b.html

DEDICATED TO THE HEROS AND HEROINES OF INTELLIGENCE OPERATIONS

REFERENCES PART 1

Greenberg, J. (2014). *Gordon Welchman: Bletchley Park's Architect of Ultra Intelligence*. Frontline Books.

Koorm, R. (2020) *Backing Bletchley: The Codebreaking Outstations, from Eastcote to GCHQ.* Amberley Publishing.

McKay, S. (2012). *The Secret Listeners: How the Y Service Intercepted the German Codes for Bletchley Park*. Aurum Press Limited.

Smith, M. (2015). *The Debs of Bletchley Park and Other Stories*. Aurum Press Limited.

Welchman, G. (1982). *The hut six story: breaking the enigma codes* (p. 326). New York: McGraw-Hill.

REFERENCES PART 2

[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

THE SARNOFF COLLECTION

WELCOME! Check for Hours

https://davidsarnoff.tcnj.edu/visit