SDR - Radio Definiowane Programowo: spoofing i zagłuszanie pasm radiowych w praktyce - GPS/WIFI/ISM.

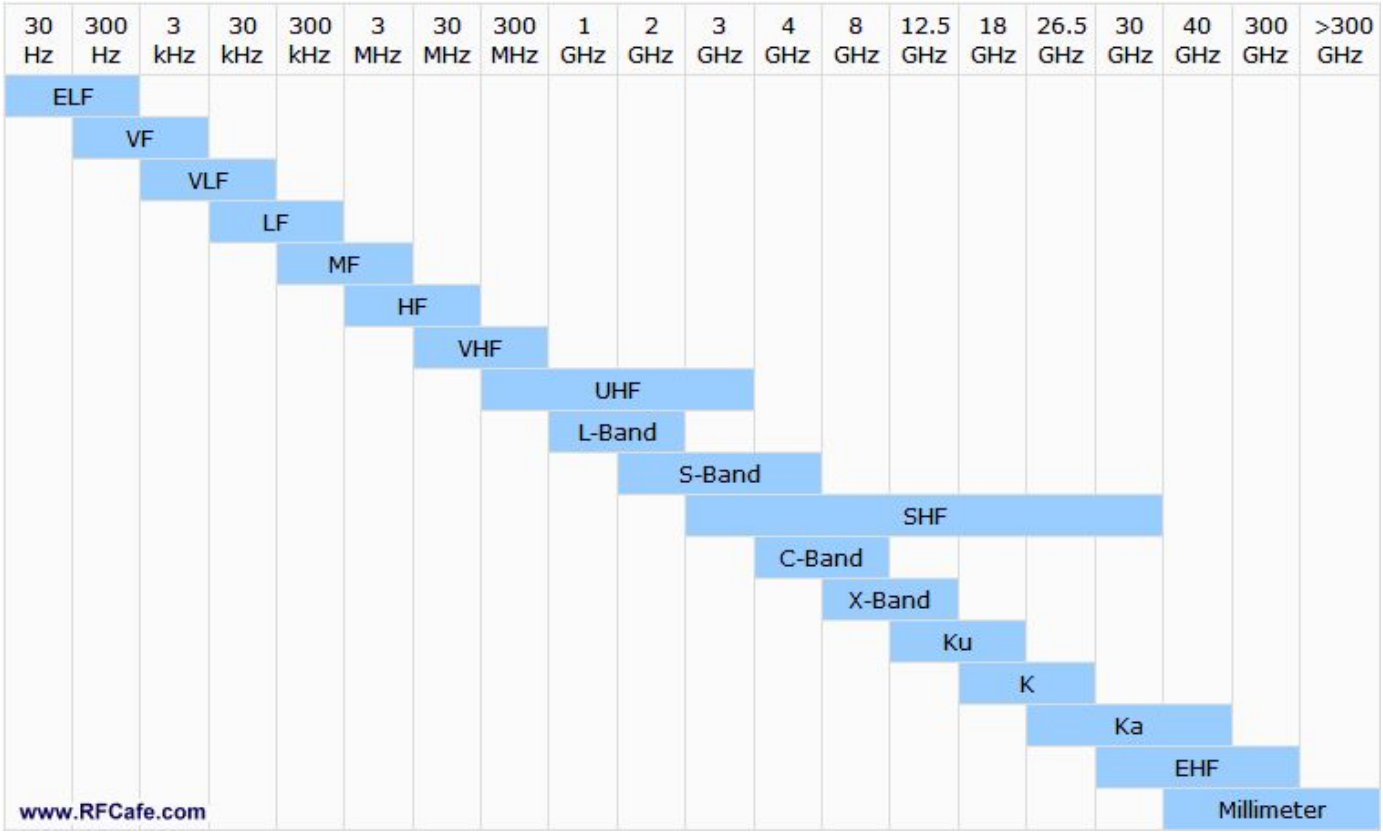
DoktorTronik

ELEKTRONIKA - SZKOLENIA - DOŚWIADCZENIE

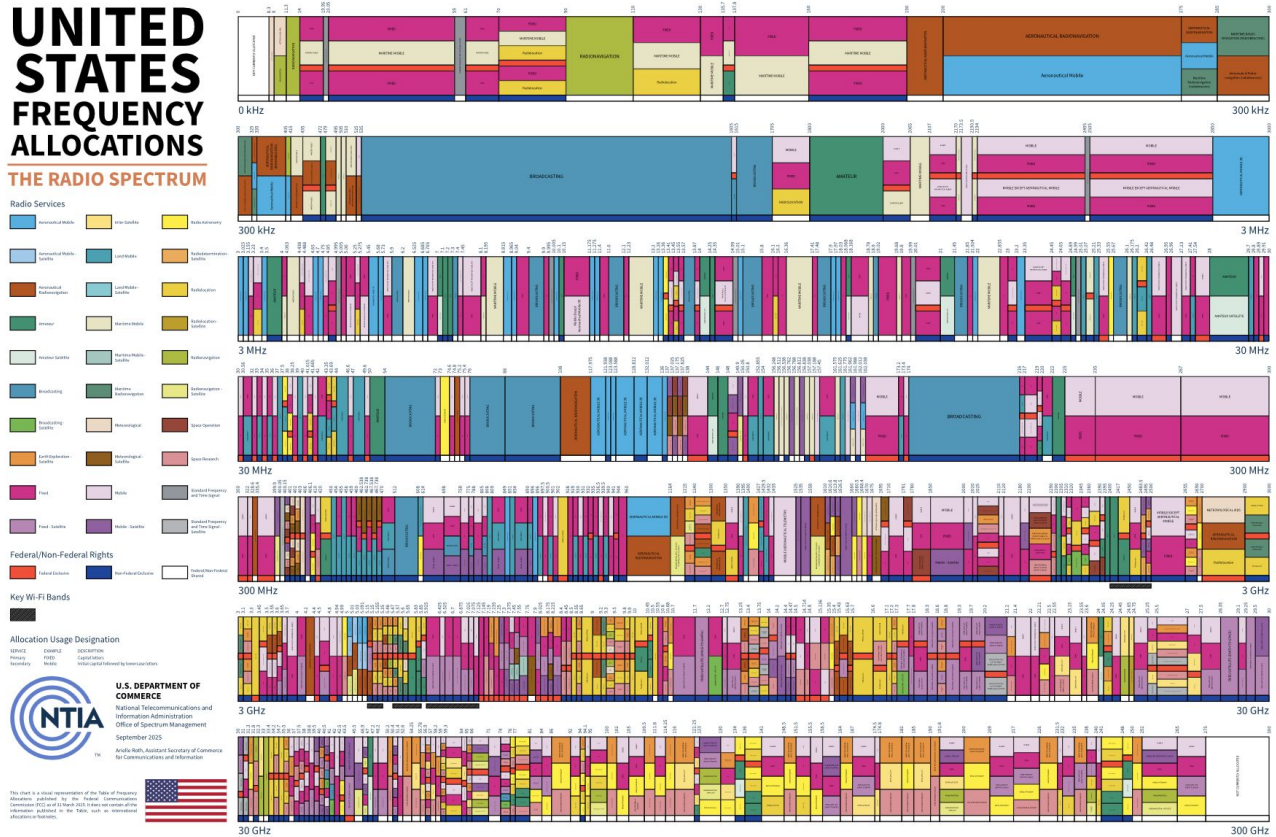
DR INŻ. RAFAŁ STĘPIEŃ

Pasma radiowe

Pasma radiowe



Pasma radiowe

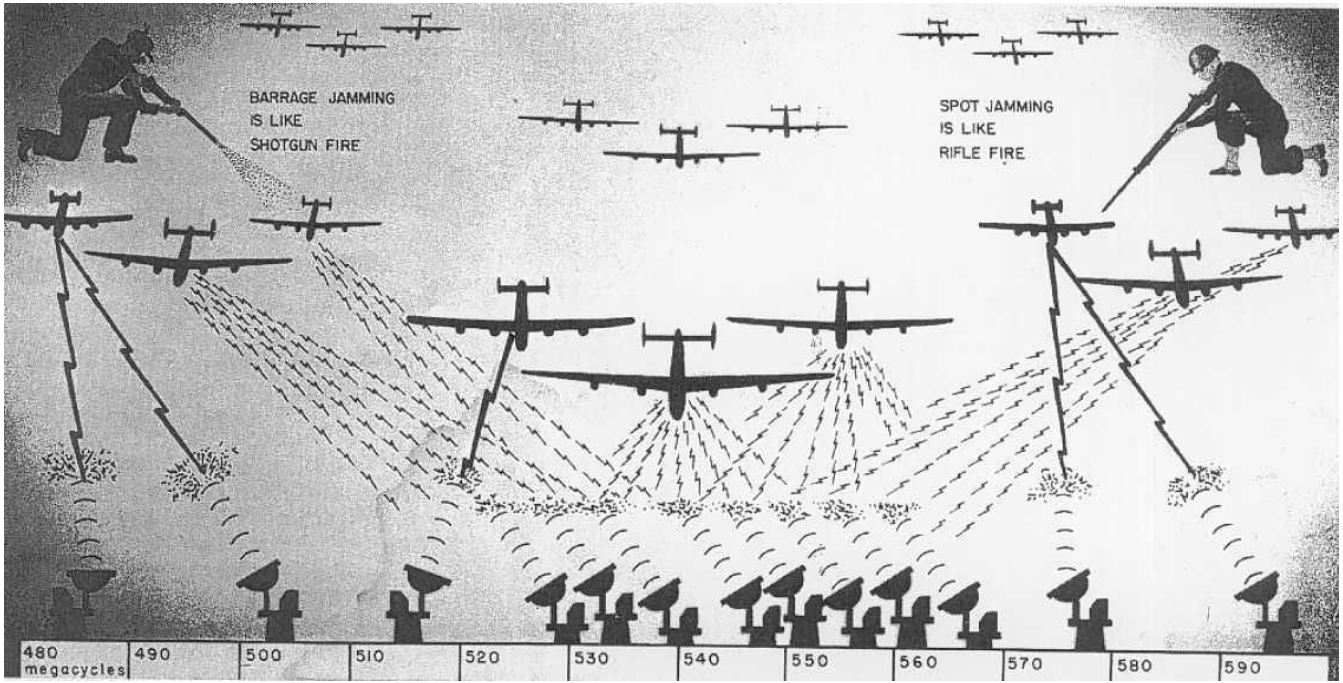


https://www.ntia.gov/sites/default/files/2025-09/ntia-us-frequency-allocations.pdf

Podstawy zagłuszania pasm radiowych

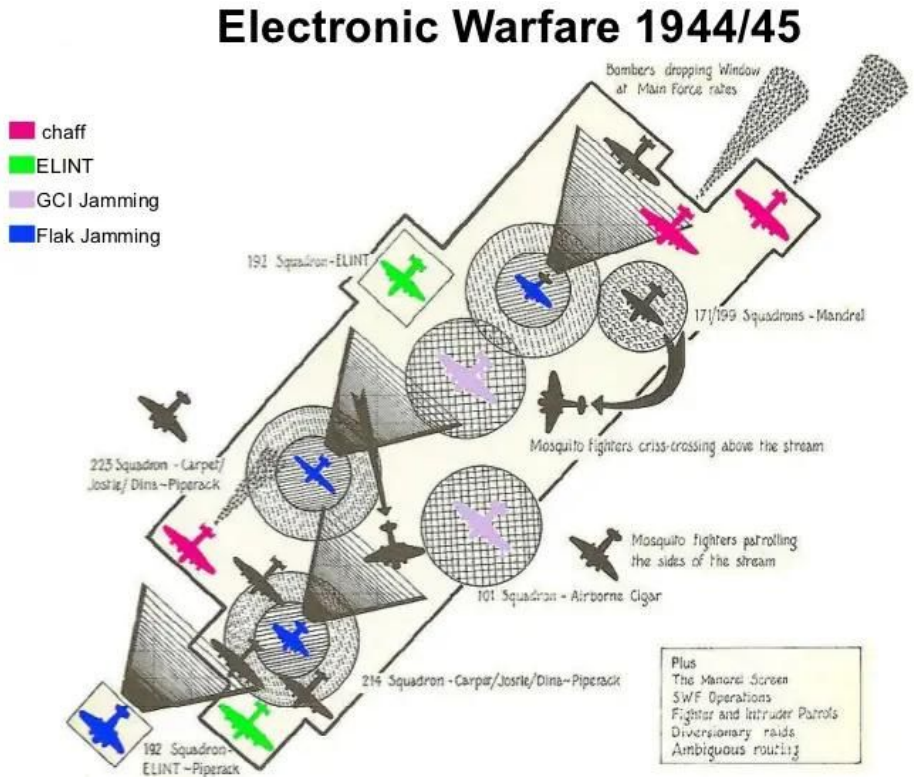
Podstawy zagłuszania pasm radiowych

1) Rys historyczny
   a) pierwsze udokumentowane zagłuszanie pasm radiowych - I Wojna Światowa
   b) II wojna światowa - zakłócenia radarów, operacja “Window”
   c) zimna wojna - kwestie propagandowe



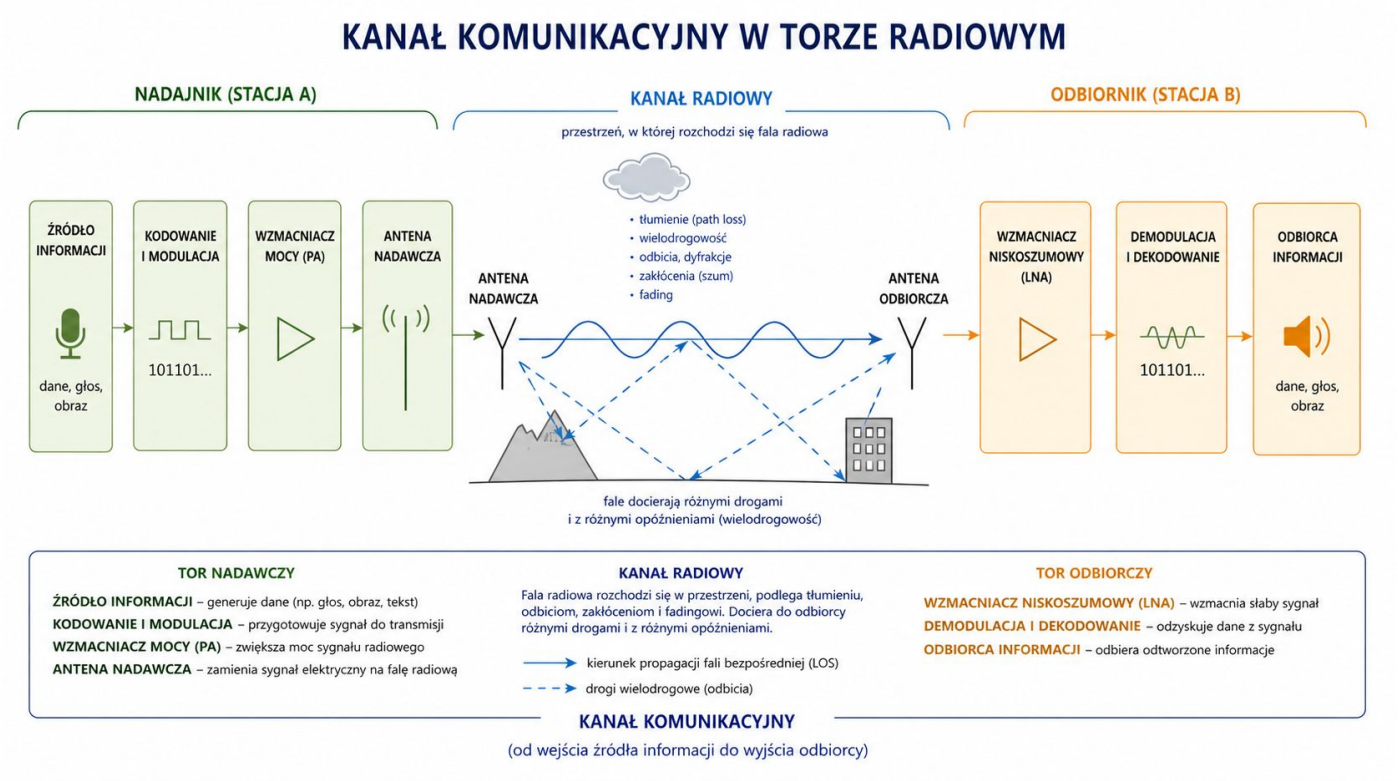
Podstawy zagłuszania pasm radiowych

Chaff - wypuszczanie paski folii w powietrzu
ELINT (*Electronic Intelligence*) - analiza parametrów sygnałów
GCI - Ground Controller Interception (nadawanie sygnałów o dużej mocy)



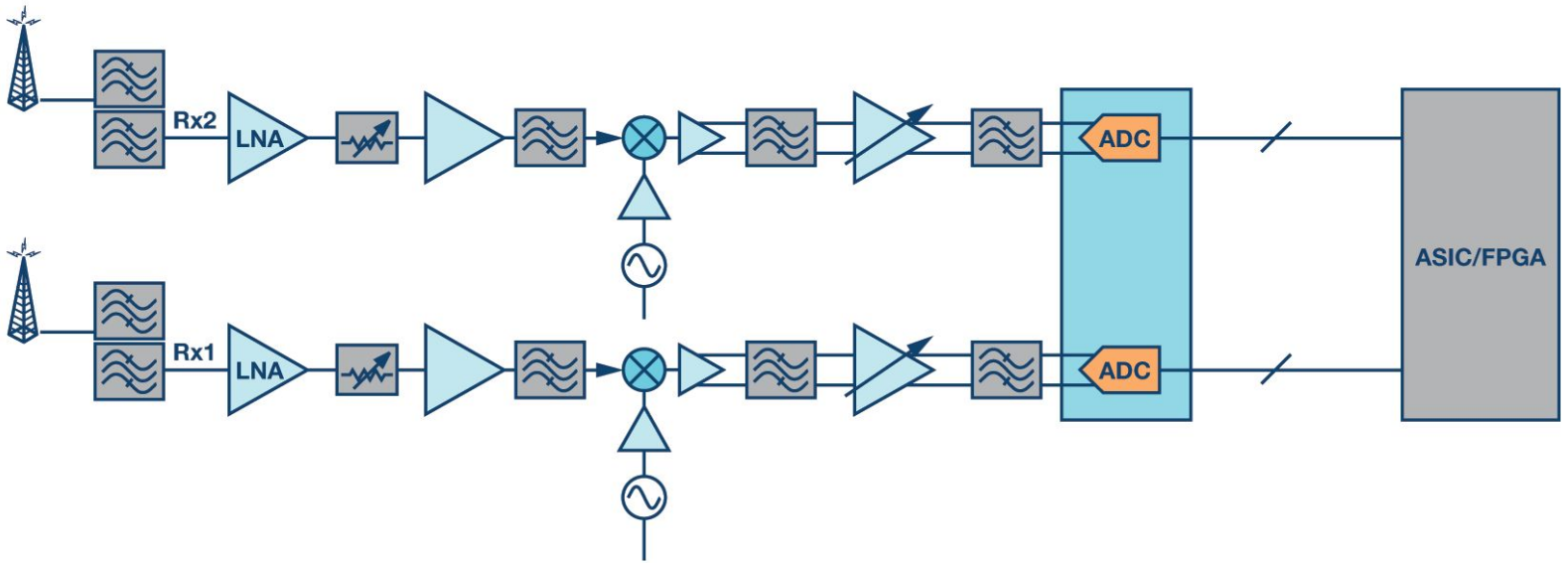
Podstawy zagłuszania pasm radiowych

1) Kanał komunikacyjny



Podstawy zagłuszania pasm radiowych

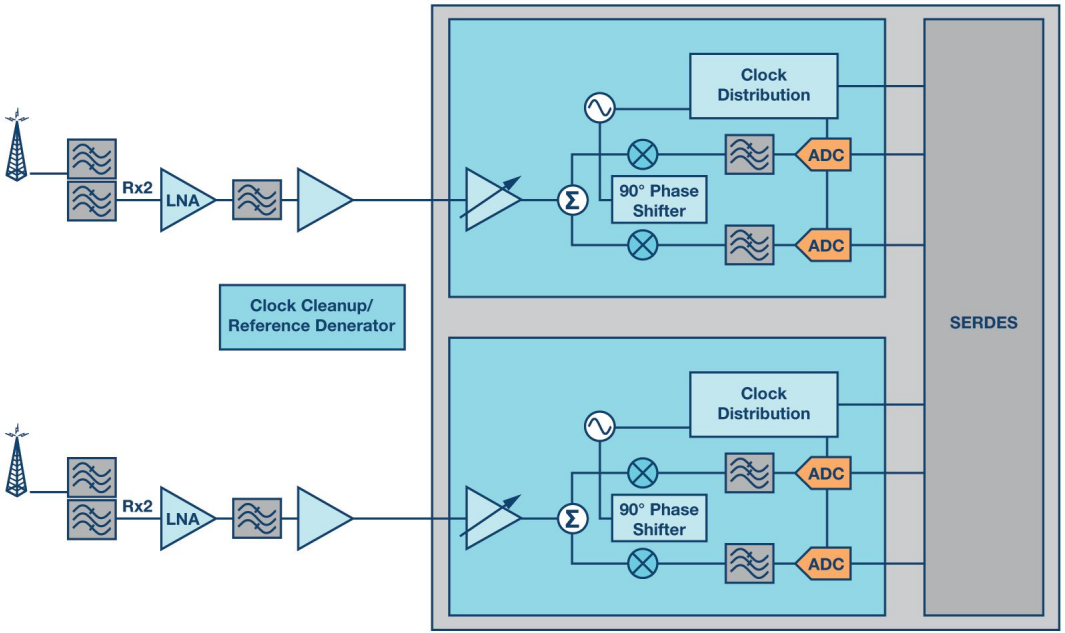
1) Budowa toru odbiorczego



https://www.analog.com/en/resources/analog-dialogue/articles/where-zero-if-wins.html

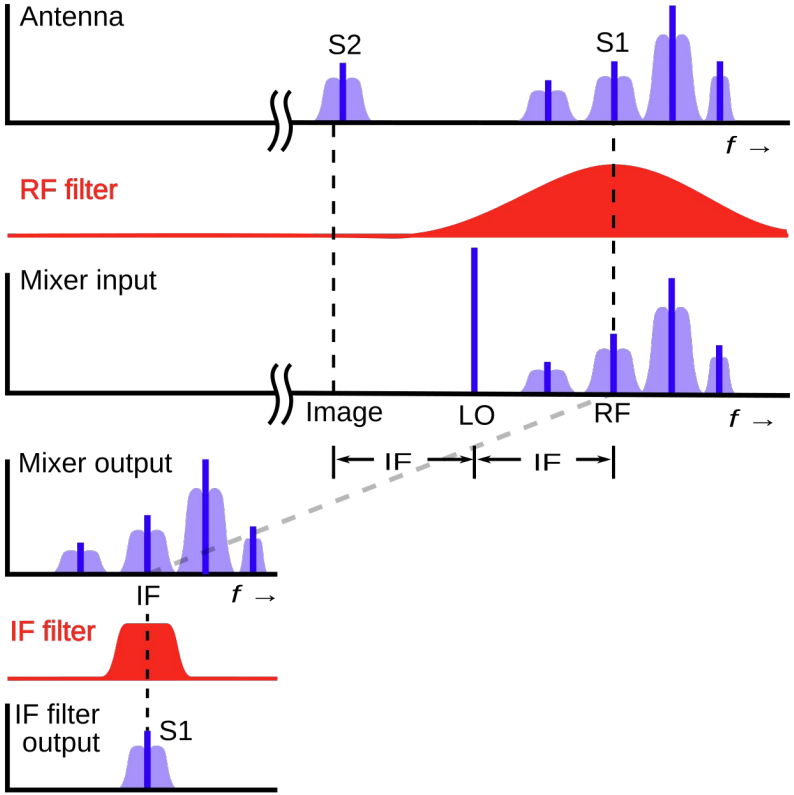
Podstawy zagłuszania pasm radiowych

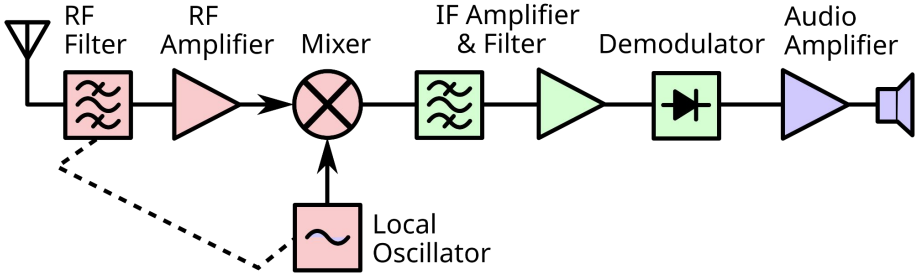
1) Budowa toru odbiorczego



https://www.analog.com/en/resources/analog-dialogue/articles/where-zero-if-wins.html

Podstawy zagłuszania pasm radiowych





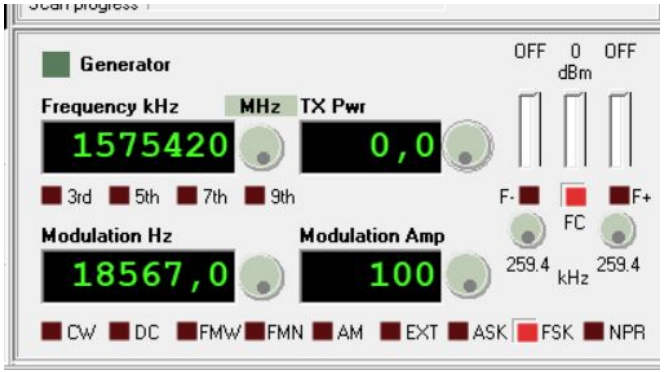
https://en.wikipedia.org/wiki/Superheterodyne_receiver

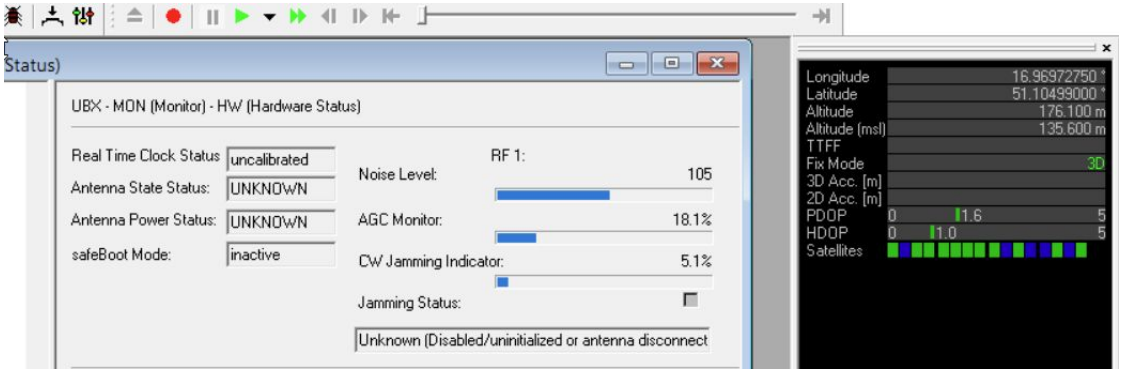
Podstawy zagłuszania pasm radiowych

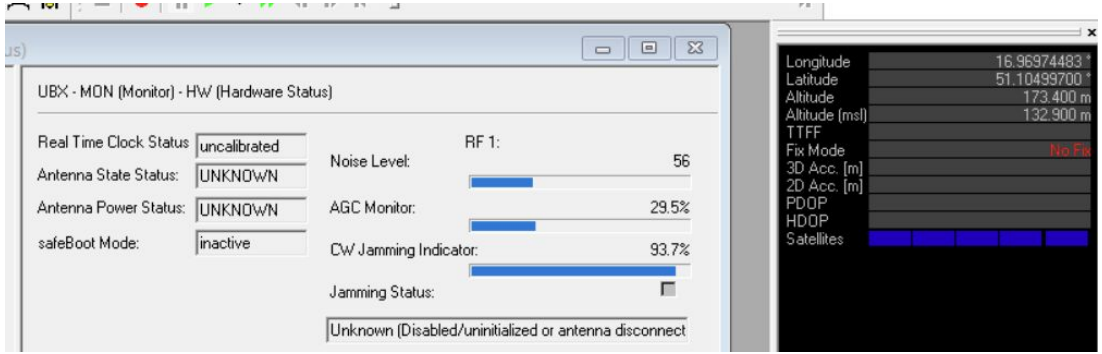
1) Zaszumianie Noise Jamming
    a) nadawanie szerokopasmowego szumu, przeważnie o dużej mocy
2) Podszywanie się - Spoofing
    a) wysyłanie błędnych sygnałów odbieranych przez odbiorniki
        i) ciekawostka: w trakcie Drugiej Wojny Światowej operatorzy naziemni nadawali komunikaty do wrogich pilotów w ich języku
3) Folia zagłuszająca (Chaff Jamming)

Przykłady zagłuszania

GPS Jamming

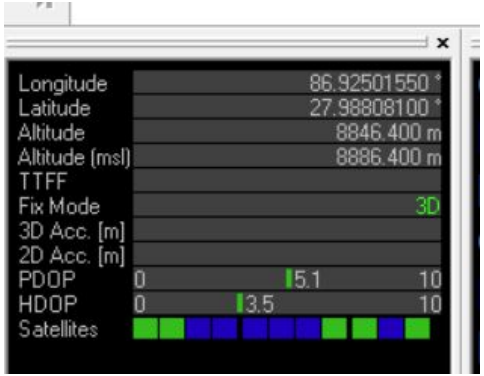

Generator
OFF 0 OFF
dBm
Frequency kHz
MHz
TX Pwr
1575420
0,0
3rd 5th 7th 9th
F- FC F+
Modulation Hz
Modulation Amp
18567,0
100
259.4
kHz
259.4
CW DC FMW FMN AM EXT ASK FSK NPR

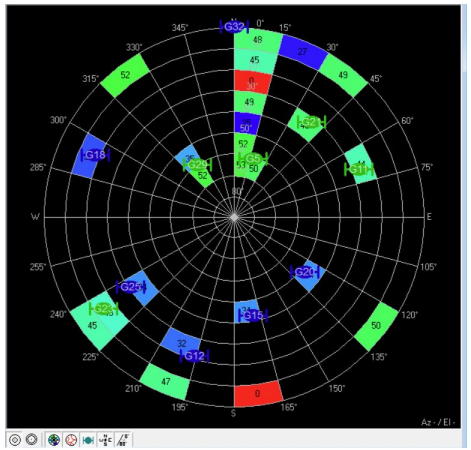

Status)
UBX - MON (Monitor) - HW (Hardware Status)
Real Time Clock Status uncalibrated
Antenna State Status: UNKNOWN
Antenna Power Status: UNKNOWN
safeBoot Mode: inactive
RF 1:
Noise Level: 105
AGC Monitor: 18.1%
CW Jamming Indicator: 5.1%
Jamming Status:
Unknown (Disabled/uninitialized or antenna disconnect
Longitude 16.96972750
Latitude 51.10499000
Altitude 176.100 m
Altitude (msl) 135.600 m
TTFF
Fix Mode 3D
3D Acc. [m]
2D Acc. [m]
PDOP 0 1.6 5
HDOP 0 1.0 5
Satellites

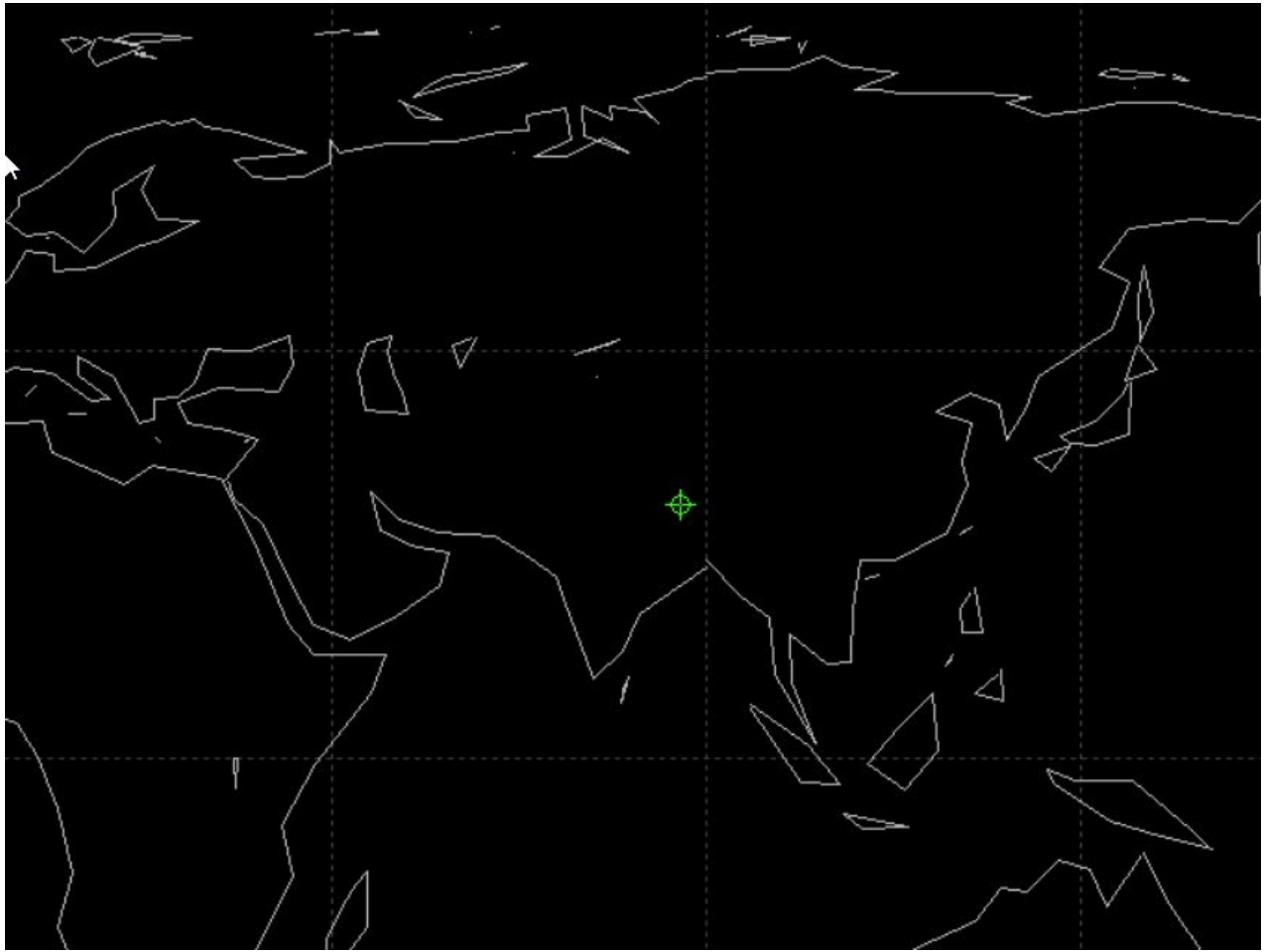

UBX - MON (Monitor) - HW (Hardware Status)
Real Time Clock Status uncalibrated
Antenna State Status: UNKNOWN
Antenna Power Status: UNKNOWN
safeBoot Mode: inactive
RF 1:
Noise Level: 56
AGC Monitor: 29.5%
CW Jamming Indicator: 93.7%
Jamming Status:
Unknown (Disabled/uninitialized or antenna disconnect
Longitude 16.96974483
Latitude 51.10499700
Altitude 173.400 m
Altitude (msl) 132.900 m
TTFF
Fix Mode No Fix
3D Acc. [m]
2D Acc. [m]
PDOP
HDOP
Satellites

GPS Spoofing

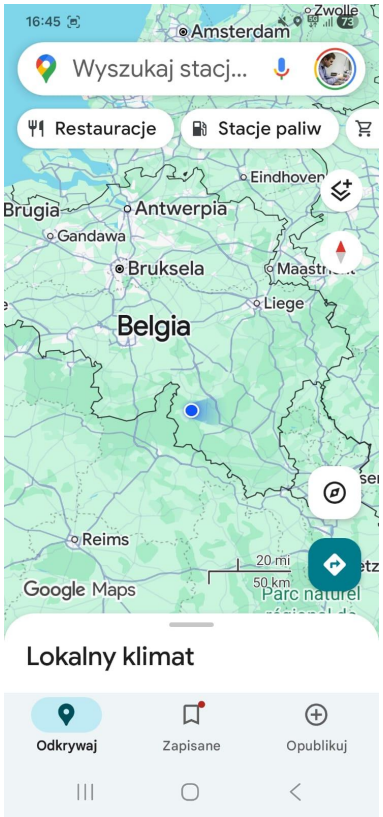
GPS Spoofing

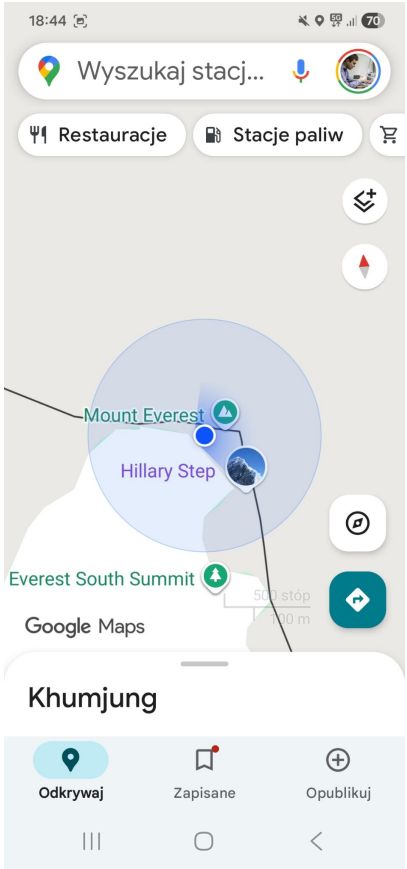


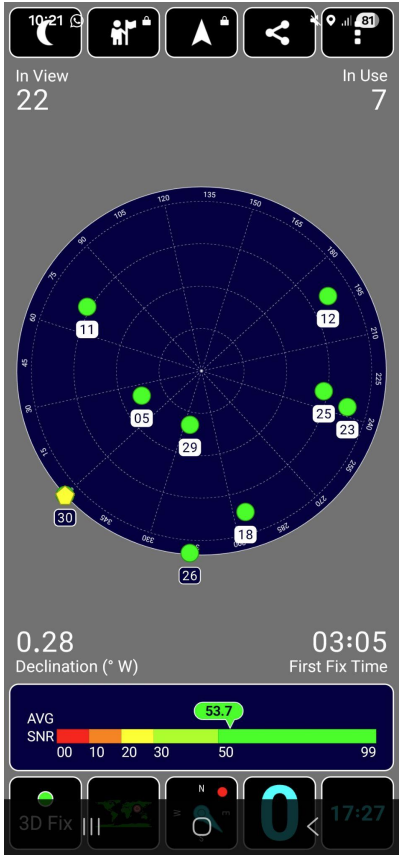




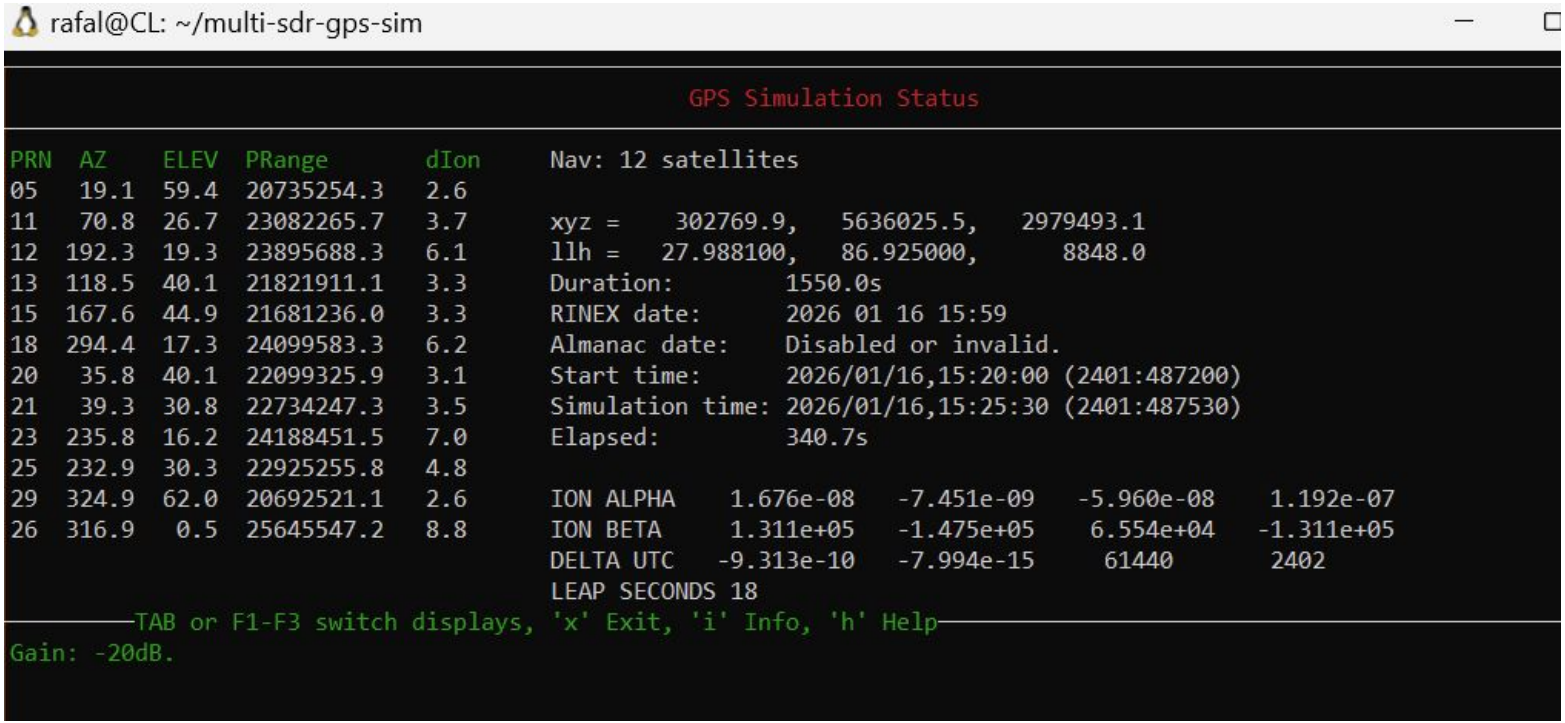
GPS Spoofing







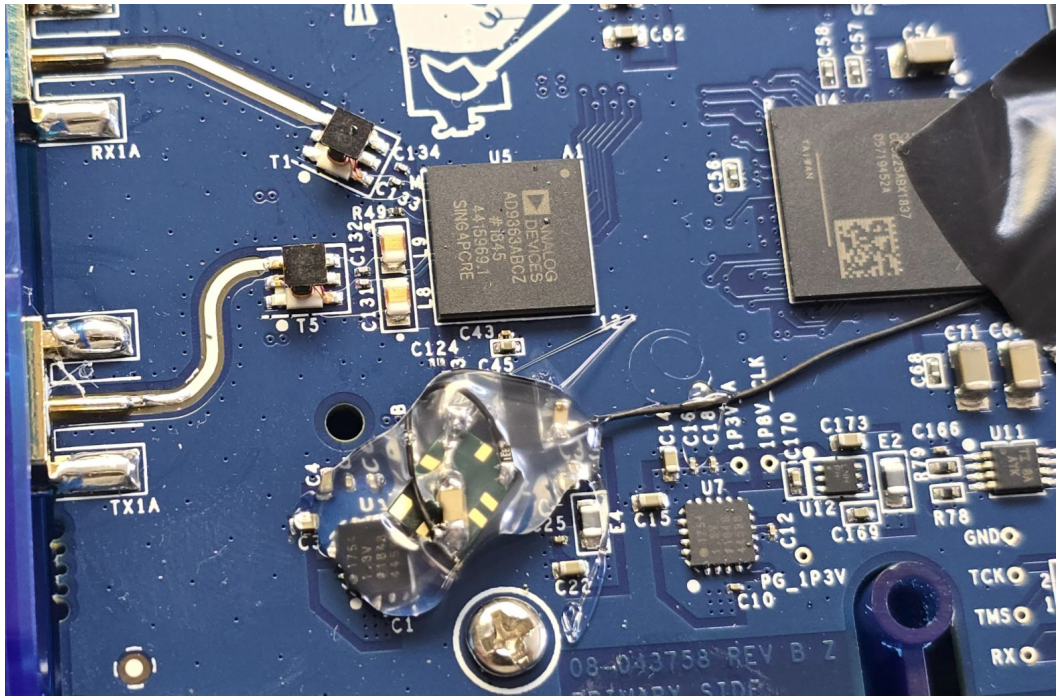
GPS Spoofing



https://github.com/Mictronics/multi-sdr-gps-sim

GPS Spoofing

Wymiana oscylatora 40MHz w Adalm Pluto



GPS Spoofing

Low Noise and Low Jitter XO

rakon
synchronising connectivity

RXO3225M

1.0 Specification References

Parameter		Description
a.	Rakon part number	513371
b.	Description	RXO3225M 40.000 MHz
c.	Document ID	RXO3225M-08

2.0 Absolute Maximum Rating [1]

Parameter		Min.	Max.	Unit
a.	Power supply	-0.5	+4.2	V
b.	Storage temperature	-55	125	°C

3.0 Frequency Characteristics

Parameter		Min.	Typ.	Max.	Unit	Test Condition / Description
a.	Nominal frequency		40.000		MHz	
b.	Temperature range	-40		85	°C	
c.	Frequency stability			±25	ppm	Including initial calibration, temperature range, supply variation and load variation
d.	Long term stability			±3 ±1	ppm ppm/yr	First year, at 25°C After first year, at 25°C

FT2MN

2.5mm x 2.0mm
TCXO

FOX

Features

- Both continuous & fixed Vdd options available
- Output waveform clipped sinewave
- Hermetically seam-sealed ceramic package
- Low current consumption

STANDARD SPECIFICATIONS[1]	
PARAMETERS	**MAX (Unless otherwise noted)**
Frequency Range (F_O)	10.000 ~ 52.000MHz
Temperature Range	
Operating (T_{OPR})	-40°C ~ +85°C (See part numbering guide below)
Storage (T_{STG})	-40°C ~ +85°C
Frequency Stability vs:	
Over Tolerance (Pre-reflow)	±1.0 PPM (Reference to fo, at 25°C±2°C)
Over Tolerance (24 hrs after reflow, 2x)	±2.0 PPM (Reference to fo, at 25°C±2°C)
Over Temperature Range[2]	±2.5 PPM (See part numbering guide below)
Over Supply Voltage Change (V_{DD}±5%)	±0.2 PPM (Vdd ± 5%)
Over Load Change [1kΩ//1pF]	±0.2 PPM (CL ± 1kΩ//±1pF)
Supply Voltage (V_{DD})	1.68V ~ 3.63V (See part numbering guide below)
Input Current (I_{DD})	
10.0 ~ 26.0MHz	2.0 mA

WiFi Jamming

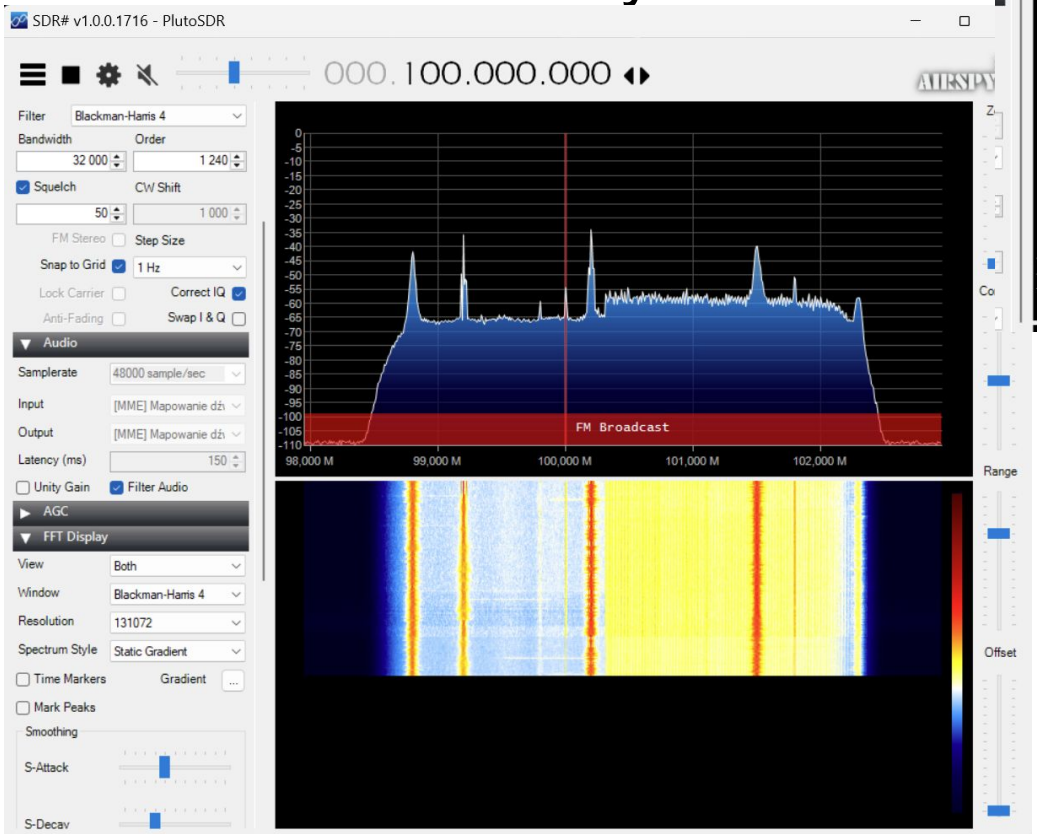
WiFi Jamming

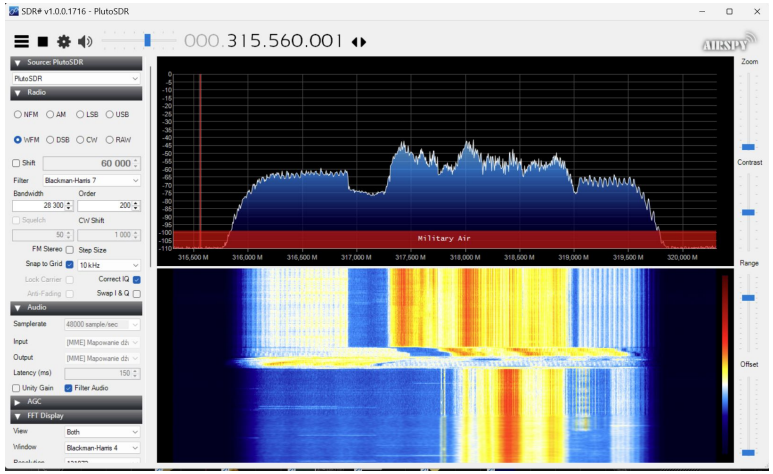
```
Reply from 91.236.131.78: bytes=32 time=34ms TTL=51
Reply from 91.236.131.78: bytes=32 time=17ms TTL=51
Reply from 91.236.131.78: bytes=32 time=17ms TTL=51
Reply from 91.236.131.78: bytes=32 time=23ms TTL=51
Reply from 91.236.131.78: bytes=32 time=35ms TTL=51
Reply from 91.236.131.78: bytes=32 time=37ms TTL=51
Reply from 91.236.131.78: bytes=32 time=19ms TTL=51
Reply from 91.236.131.78: bytes=32 time=34ms TTL=51
Reply from 91.236.131.78: bytes=32 time=17ms TTL=51
Request timed out.
Reply from 91.236.131.78: bytes=32 time=2697ms TTL=51
Reply from 91.236.131.78: bytes=32 time=21ms TTL=51
Reply from 91.236.131.78: bytes=32 time=34ms TTL=51
Reply from 91.236.131.78: bytes=32 time=1262ms TTL=51
Reply from 91.236.131.78: bytes=32 time=21ms TTL=51
Reply from 91.236.131.78: bytes=32 time=20ms TTL=51
Reply from 91.236.131.78: bytes=32 time=2253ms TTL=51
Reply from 91.236.131.78: bytes=32 time=20ms TTL=51
Reply from 91.236.131.78: bytes=32 time=25ms TTL=51
Request timed out.
Reply from 91.236.131.78: bytes=32 time=3736ms TTL=51
Reply from 91.236.131.78: bytes=32 time=20ms TTL=51
Reply from 91.236.131.78: bytes=32 time=18ms TTL=51
Reply from 91.236.131.78: bytes=32 time=1028ms TTL=51
Reply from 91.236.131.78: bytes=32 time=22ms TTL=51
Reply from 91.236.131.78: bytes=32 time=106ms TTL=51
Reply from 91.236.131.78: bytes=32 time=43ms TTL=51
Reply from 91.236.131.78: bytes=32 time=18ms TTL=51
Reply from 91.236.131.78: bytes=32 time=104ms TTL=51
```

Pasmo sieciowe (kanał):	5 GHz (44)
Zagregowana szybkość łącza (odbieranie/przesyłanie):	1081/600 (Mbps)

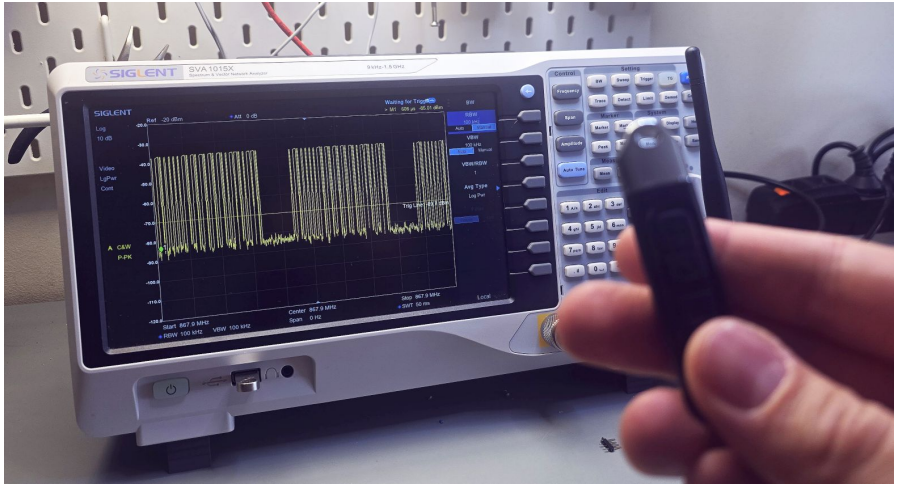
Podsłuchiwanie danych

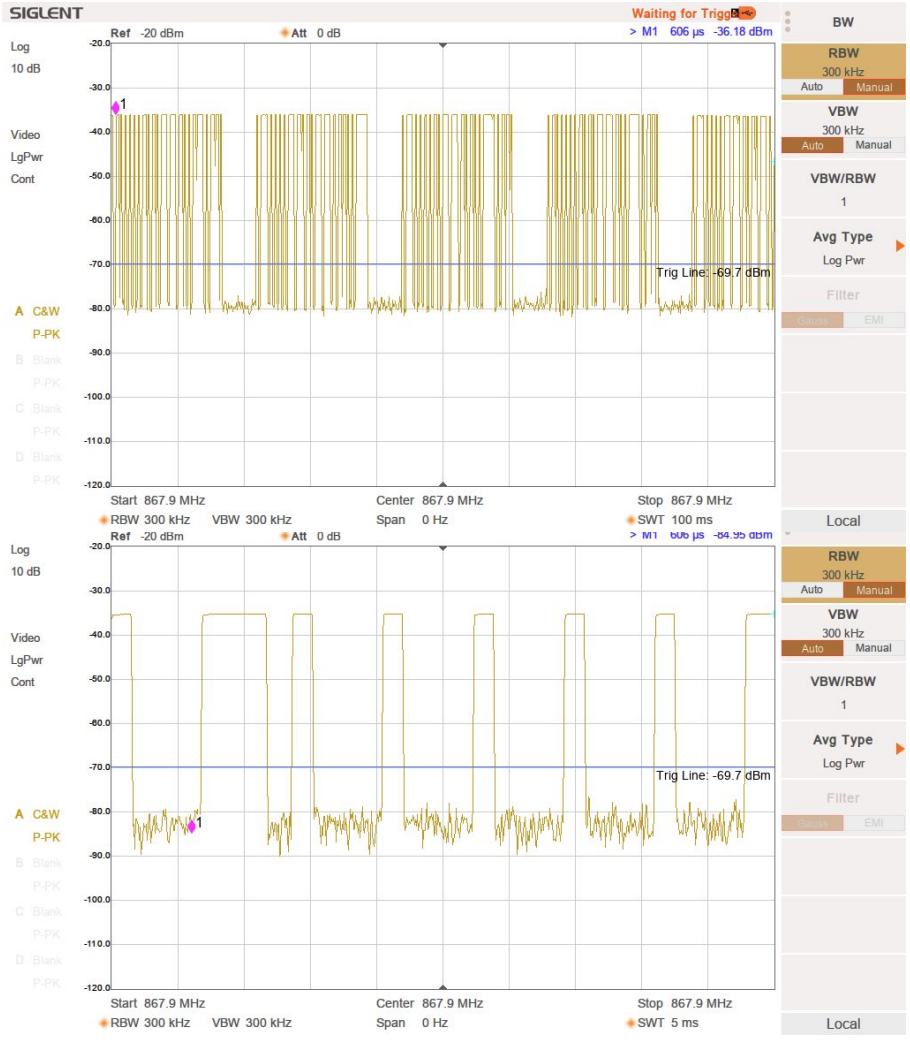
Podsłuchiwanie danych



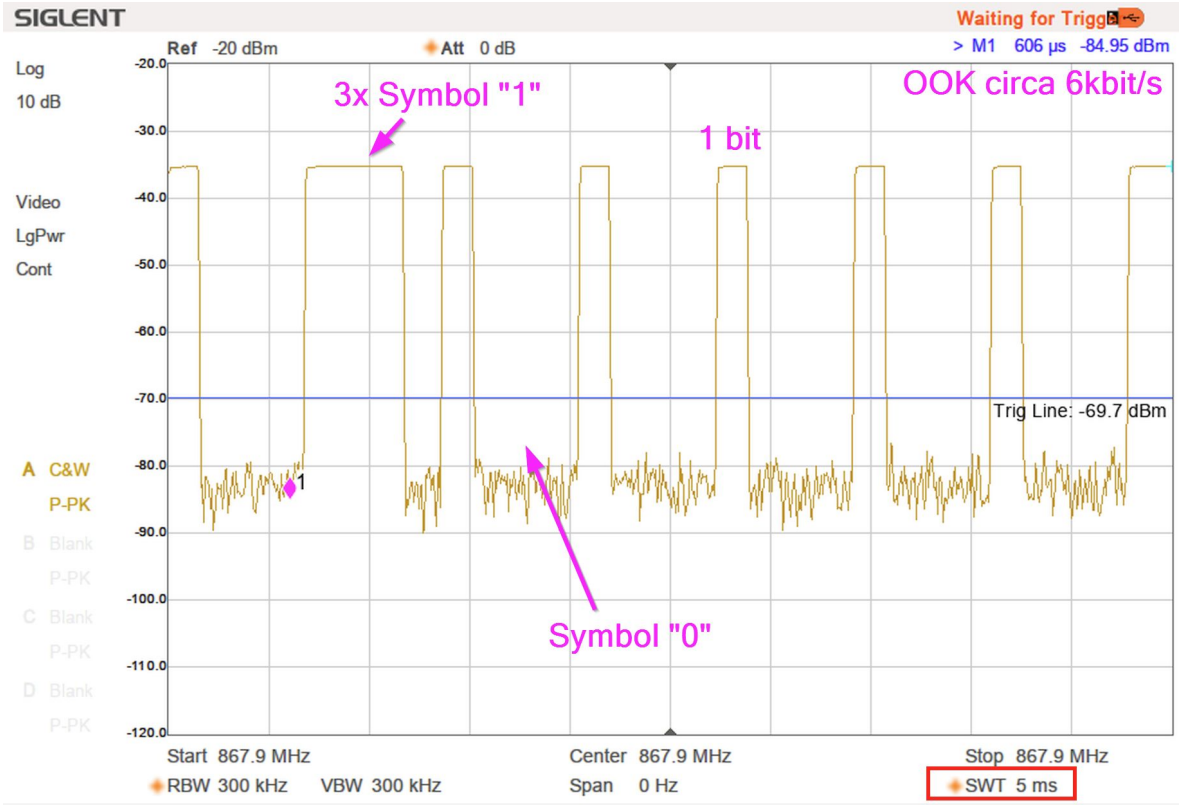


Podsłuchiwanie danych





Podsłuchiwanie danych



Podsumowanie

Podsumowanie

1) Zakłócanie pracy systemów radiowych jest możliwe na kilka sposobów
   a) Noise Jamming
   b) Spoofing
2) Technika SDR pozwala na generowanie różnych sygnałów radiowych w szerokim spektrum częstotliwości
3) Z wykorzystaniem analizatora widma możliwe jest dekodowaine i analiza ramek danych prostych systemów ISM/RKE

Koniec