What The H@CK 2019

RADIO!
Trochę historii
Radioamatorstwo/krótkofalarstwo
Jak zacząć?
Jak to się ma do bezpieczeństwa :)

Link do prezentacji:
https://github.com/sq5bpf/misc/blob/master/wth2019.pdf

Jacek Lipkowski SQ5BPF

~$ whoami

- Jacek Lipkowski

  Hobby:
- Krótkofalarstwo. Znak SQ5BPF

  (od ponad 25 lat, licencja z roku 1993)
- Unixy, sieci. I ich psucie :) (od ponad 20 lat)
- Elektronika (od zawsze)

  Pracuje w Pekao Financial Services Sp. z o.o.

  Prezentacja ta jest moja i nie wyraża poglądów pracodawcy.

Co jest w prezentacji

Radio to obecnie modny temat w bezpieczeństwie :)

- Trochę historii radia
- O krótkofalarstwie
- Sugestie jak można zacząć z radiem (i SDR)
- Linki, słowa kluczowe (do dalszego zgłębiania tematu)

Każdy z tych tematów zasługuje na osobny wykład, więc niestety zostaną one potraktowane bardzo skrótowo.

Trochę Historii

Trochę historii: początki

James Clerk Maxwell opisał teorię fal elektromagnetycznych w 1861 roku:

10 Zmienne pole elektryczne wytwarza pole magnetyczne

20 Zmienne pole magnetyczne wytwarza pole elektryczne

30 GOTO 10

:)

Trochę historii: początki 2

Heinrich Hertz pokazał implementację praktyczną 1886 rok:

- „Antena” ładowana ze źródła wysokiego napięcia
- Przeskok iskry w iskierniku powoduje zwarcie, i przez to nagłą zmianę pola elektrycznego
- Detektor w postaci pętli przeciętej w środku z iskiernikiem. Detekcja zmiennego pola magnetycznego. Zasięg rzędu metrów.

„Nie sądzę, że fale bezprzewodowe, które odkryłem, będą miały praktyczne zastosowanie. To jest tylko eksperyment mający pokazać że mistrz Maxwell miał rację ...” - Heinrich Hertz

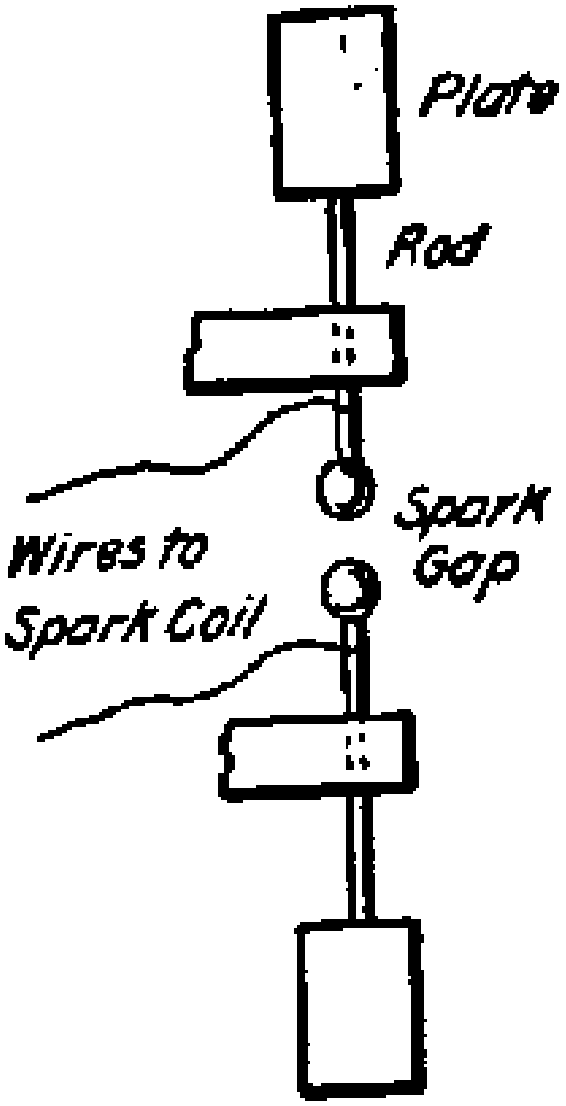
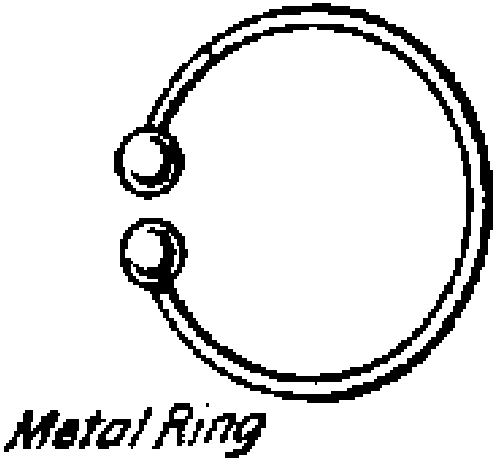


Plate
Rod
Spark Gap
Wires to Spark Coil


Metal Ring

Trochę historii: początki 3

Wkraczają amatorzy (nie wiedzą że czegoś się nie da zrobić), m.in. Marconii

- Ma dużo czasu, „omija” obowiązkową służbę wojskową (lifehack: rejestruje się jako ochotnik i prosi o zawieszenie służby :)
- Zamiast anteny w postaci dwóch przewodów używa uziemienia i długiego drutu
- Koherer jako detektor
- Głównie zbiór pomysłów innych

Zasięg parę km (1895 rok), wzgórze pomiędzy obiornikiem i nadajnikiem.

Włosi niezainteresowani, ale zna angielski, więc próbuje w Wielkiej Brytanii.

W 1899 wysyłał już sygnał przez kanał La Manche (co zagraża monopolowi przedsiębiorców posiadających podwodne kable telegraficzne).

https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6529378

Trochę historii: początki 4

Wiele osób prowadziło podobne badania, ale to Marconi „zmonopolizował” radio – vendor lockin

Pierwszy hack radiowy podczas demonstracji Marconiego w Royal Instituition w Londynie – 1903. „Bezpieczny system wysyłania sygnałów”

„There was a young man from Italy, who diddled the public quite prettily. RATS RATS RATS RATS ...” - Nevil Maskelyne

Vendor lockin: Marconi International Marine Communication Company – outsourcing łączności radiowej (dawali stację i radiooperatora). Radiooperator ma zakaz robienia łączności ze stacjami innych firm. Problem m.in. podczas katastrofy RMS Titanic

Trochę historii: wkraczają amatorzy!

W Europie technika radiowa jest mocno kontrolowana (odbiór też), mało śladów historycznych.

W USA jest „wolna amerykanka” (co nie jest zabronione jest dozwolone):

- Publikacje w prasie popularnonaukowej.
- Generator wysokiego napięcia (cewka zapłonowa od Forda T)
- Baterie/akumulatory jako zasilanie
- Detektory elektrolityczne albo kryształkowe (nie wiadomo jak działają, ale działają :)
- Dziesiątki tysięcy stacji (hobby młodych chłopców).
- Nie do konca wiedzą że czegoś się nie da zrobić (więc to robią)

Trochę historii: amatorzy 2

Amatorzy w USA przeszkadzają stacjom profesjonalnym (tu pewnie było dużo niedokumentowanych hacków :).

Radio Act of 1912: Licencjonownie dostępu do widma radiowego:

„Służba radioamatorska”.

Ograniczenie do fal krótszych niż 200m (czyli powyżej 1.5 MHz): „nie wyjdą poza swój ogródek”.

Amatorzy wkrótce odkrywają że fale krótkie nie są aż takie bezużyteczne.

Pierwsze legalne łączności USA-Europa w 1921 roku.

Wcześniejsze próby w Europie niestety głównie nieudokumentowane.

Służba radioamatorska

- Trzeba zdać egzamin organizowany przez UKE.
- Obecnie bardzo prosty – RÓBCIE LICENCJE !!!1!
- Ma wydzielone pasma „do zabawy” (np. 136kHz, 3.5MHz, 144MHz, 10GHz i wiele innych) i spory limit mocy (500W mocy nadajnika dla większości pasm).
- Każdy dostaje unikalny w skali światowej znak wywoławczy (mój: SQ5BPF)

Mogą używać urządzeń własnej konstrukcji, oraz hackować urządzenia fabryczne.

Bez homologacji :)

Jest to doskonały wstęp do przygody z radiem.

Nie potrzebujemy licencji żeby słuchać za pomocą odbiornika („urządzenie przeznaczone wyłącznie do odbioru”).

„Nasłuchowcy” (wedle terminologii krótkofalarskiej)

Nasłuch w Polsce

- Nie wymaga pozwolenia używanie urządzeń radiowych przeznaczonych wyłącznie do odbioru. Art 144 pkt 1 Pr. Telekomunikacyjne. *(Nie słuchamy za pomocą urządzenia które może nadawać)*

- Art. 267

  § 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

  § 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.

  § 3.Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.
- § 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1-3 ujawnia innej osobie. *(Jeśli już przez przypadek czegoś się dowiemy to nie ujawniamy dalej ~~osobiście~~).*
- § 5. Ściganie przestępstwa określonego w § 1-4 następuje na wniosek pokrzywdzonego. *(Jeśli ktoś nie wie że jest monitorowany to nie może zgłosić się jako „pokrzywdzony”).*

Nasłuch

- Każdy system telekomunikacyjny można nasłuchiwać jeśli znamy parametry (np od kolegi kolegi :) i zaprogramujemy we własym radiotelefonie. Łamie art 144 i art 267 (nie polecam, podłączenie do sieci). Realny problem w wielu sieciach.

- Art 267 § 4: jeśli już się czegoś przypadkowo posłuchało to nie można tego ujawniać innym.

- Z tego powodu jest mało publicznie dostępnych informacji na tematy bezpieczeństwa radia (przynajmniej z Polski). Ta prezentacja też jest pozbawiona „pikantnych szczegółów”. Nie wiadomo czego nie można przekazywać dalej (głos, może identyfikatorów stacji w sieci, a może np. same parametry sieci, a może nawet sama częstotliwość).

- Duże pole do (nad)interpretacji. Nie polecam obcowania z wymiarem sprawiedliwości (np. sprawa Włodka Gillera, któremu zarzucano m.in. ujawnienie tajemnicy państwowej)

Jak zacząć?
Czym się zainteresować na początku?

Software Defined Radio

- Kiedyś musielibyśmy zrobić lub kupić odbiornik.
- Klasyczny odbiornik (superheterodynowy, są inne): obwody wejściowe, przemiana na niższą częstotliwość, filtrowanie, demodulatory (osobny dla każdej emisji).
- Odbiornik SDR (hybrydowy): obwody wejściowe, przemiana na niższą częstotliwość, filtrowanie, przetwornik AD. Reszta w oprogramowaniu.
- Odbiornik SDR: obwody wejściowe (albo i nie), przetwornik AD. Reszta w oprogramowaniu.

- Obserwujemy tyle pasma ile ma przetwornik AD (analogowo-cyfrowy)
- Cała obróbka sygnału w oprogramowaniu (są gotowce, nie trzeba wymyślać koła od nowa), odbiór innej emisji/protokołu wymaga jedynie zmiany oprogramowania.
- Można przetwarzać wiele sygnałów w paśmie naraz
- Problem w tym że fabryczne odbiorniki SDR były drogie (np. USRP, WinRadio)

SDR :)

- Sytuacja się zmieniła. Bajecznie tanie SDR z odbiornika DVB-T
- 24-1700MHz (dla tunera R820T)
- max około 2.5MHz pasma, ADC 8-bitowy (hack używający nidokumentowanego trybu dekodera DVB-T RTL2832)
- 60zł !!! !!1!
- Dużo oprogramowania: gqrx, GNUradio, rtl_fm (pakiety np w debianie) i in. (jest też opgrogramowanie pod windows, mac os, android itp)
- 30 lat temu to byłaby ściśle kontrolowana technologia wojskowa (a teraz mamy ją za 60zł)

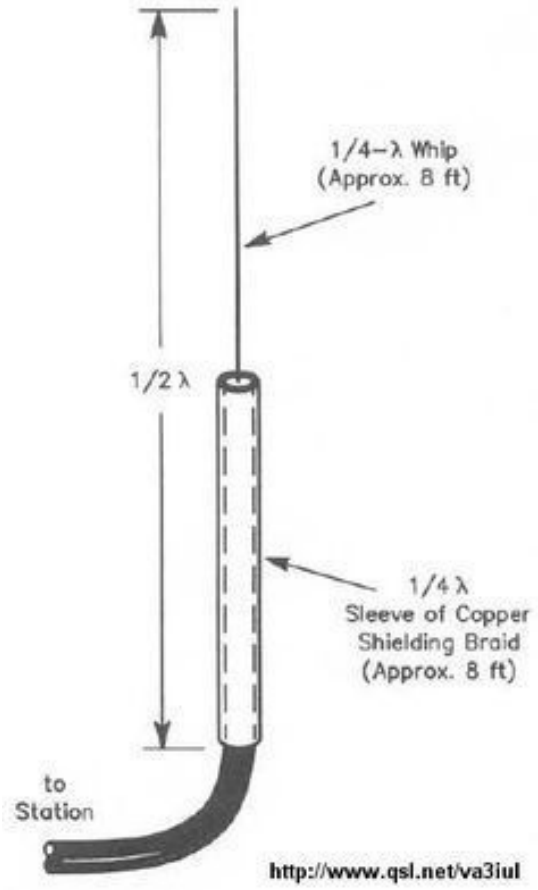
SDR (jak zacząć)

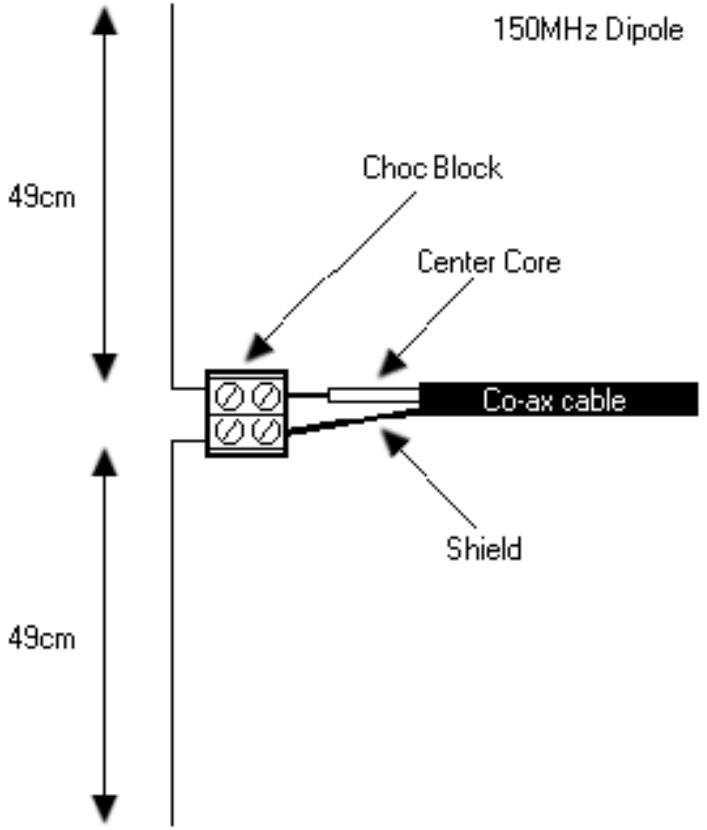
- Tuner SDR
- Komputer z gqrx (jest pakiet w debianie), odbiera popularne modulacje analogowe: AM, FM, SSB. Pod windows jest program SDR#.
- Antena. np. dipol półfalowy z 2 prętów/rurek 45cm (działa na 150MHz i w miarę dobrze na 450MHz, kompromis na te 2 pasma). Dużo opisów w internecie, można też kupić gotową.
- Kabel koncentryczny do podłączenia anteny (może być 75 omowy od TV)
- Proponuje na początek posłuchać: 108-137 MHz* AM (pasmo lotnicze), 137-174 MHz FM (potocznie VHF) , 420-470 MHz FM (potocznie UHF)
- ADS-B: 1090MHz , fabryczna antena do

  tunera skrócona do 3cm.

* https://dlapilota.pl w wyszukiwarke wpisujemy MHz

Proste anteny





Nowy wspaniały świat radia

Zawsze gdy hobbyści mogą zajrzeć tam gdzie wcześniej nie można było łatwo, to coś znajdą :)

- Promiscious mode w wifi (i frame injection)
- Urządzenia do kart RFID np. Proxmark
- I teraz radio (tryb SDR w RTL2832 odkryty w 2012 roku)
- Itp. itd…

- Protokoły często projektowane bez wnikania w bezpieczeństwo („a kto by się tam tym interesował”, „trzeba by mieć specjalistyczny sprzęt” itd. :)
- Działają „stare sztuczki”: plaintext, brak autoryzacji komunikatów (jedynie sumy kontrolne przeciw zakłóceniom), replay attack, MiTM, DoS …

Czego można nasłuchiwać?

Łączności krótkofalarskie oczywiście

- Radiofonia (nawet ta odległa)
- Wszelki ruch przeznaczony do publicznej konsumpcji: łączność samolotów, satelity pogodowe.
- Urządzenia (teraz modnie nazywane IoT)

Kolega kolegi:

- ~~Służby? Firmy? Inna łączność nieszyfrowana?~~
- Piraci

Łączności krótkofalarskie

- „Zaliczenie łączności” - przekazanie znaków, raportu (jak słyszę) i lokalizacji.
- Żucie szmat - rozmowy o wszystkim i o niczym
- Eksperymenty radiowe

  Fonia (łączność głosem)

  Telegrafia (alfabet morse’a)

  Emisje cyfrowe (komputer nadaje i odbiera)

- Propagacja (jak fala radiowa trafia od nadajnika do odbiornika): w linii prostej, przez odbicie od jonosfery, przez odbicie od księżyca, przez rozproszenie na czymś (ślady meteorytów, samoloty, krople deszczu, duża góra itp.).

I nie „tylko” zwykłe łączności

- Łączność kryzysowa SP EMCOMM

  https://emcom.pzk.org.pl/
- Bitcoin via radio

  https://www.coindesk.com/bitcoin-coders-send-international-lightning-payment-over-ham-radio

  http://kryptoradio.koodilehto.fi/
- Maile (i inne komunikaty) via radio (via ALE, jak wojsko)

  http://hflink.com/
- Łączność z Międzynarodową Stacją Kosmiczną

  https://www.ariss.org/
- Własne satelity

  https://www.amsat.org

Radiofonia (i telewizja)

Odbiór dalekich stacji radiowych (przy dobrych warunkach stacje z krajów ościennych, czasem dużo dalej). Radiofonia w zakresie fal ultrakrótkich przeznaczona jest dla zasiegu lokalnego. Zakresy fal krótkich, srednich, długich są przeznaczone do odbioru na duże odległości.

DX TV – odbiór dalekich stacji telewizyjnych (teraz utrudnione przy telewizji cyfrowej).

Czasem ciekawostki, np. stacje numeryczne na falach krótkich (nadaja zaszyfrowane komunikaty dla szpiegów, szyfrowanie one time pad, wiele osób się tym ekscytuje). http://priyom.org/

„Publiczny” ruch

- Łączność samolotów 108-137 MHz AM
- ADS-B na 1090 MHz (lokalizacja samolotów)

  https://github.com/flightaware/dump1090
- ACARS na 131.550 MHz https://www.acarsd.org/

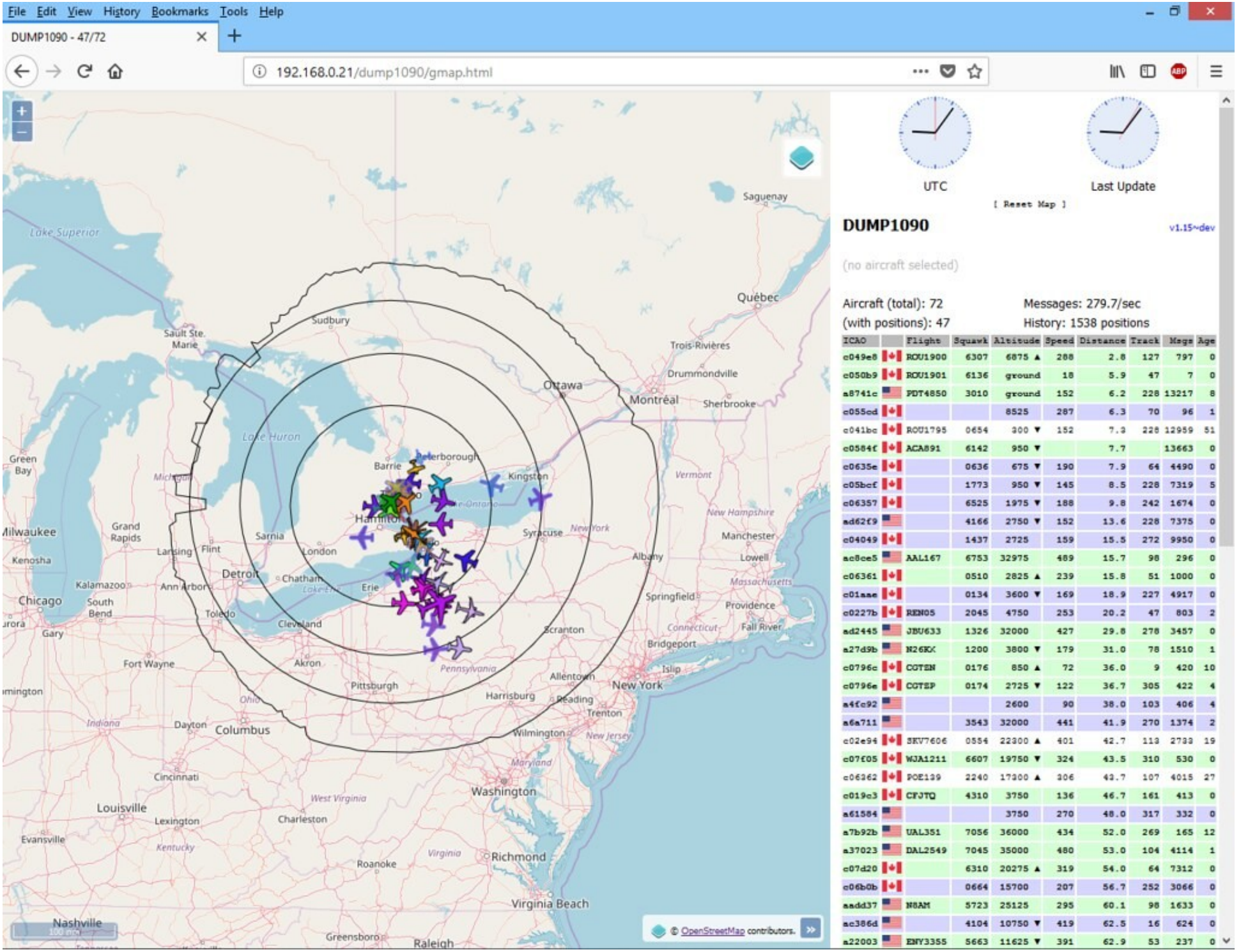
  Flight id: LX1337 [Moscow (Domodedovo), Russian Federation-Geneva, Switzerland] [Swiss International Air Lines/Crossair]

  Message content:-

  XLSZH PLS VERIFY CREDIT CARD: MASTER xxxx000101000xxxx EXP 08/12 CHF 610
- AIS (lokaliazcja statków):

  https://github.com/dgiardini/rtl-ais
- Satelity pogodowe:

  https://github.com/DrPaulBrewer/rtlsdr-automated-wxsat-capture


File Edit View History Bookmarks Tools Help
DUMP1090 - 47/72
192.168.0.21/dump1090/gmap.html
UTC
Last Update
[Reset Map]
DUMP1090
v1.15~dev
(no aircraft selected)
Aircraft (total): 72
Messages: 279.7/sec
(with positions): 47
History: 1538 positions
ICAO Flight Squawk Altitude Speed Distance Track Msgs Age
c049e8 ROU1900 6307 6875 ▲ 288 2.8 127 797 0
c050b9 ROU1901 6136 ground 18 5.9 47 7 0
a8741c PDT4850 3010 ground 152 6.2 228 13217 8
c055cd 8525 287 6.3 70 96 1
c041bc ROU1795 0654 300 ▼ 152 7.3 228 12959 51
c0584f ACA891 6142 950 ▼ 7.7 13663 0
c0635e 0636 675 ▼ 190 7.9 64 4490 0
c05bcf 1773 950 ▼ 145 8.5 228 7319 5
c06357 6525 1975 ▼ 188 9.8 242 1674 0
ad62f9 4166 2750 ▼ 152 13.6 228 7375 0
c04049 1437 2725 159 15.5 272 9950 0
ac8ee5 AAL167 6753 32975 489 15.7 98 296 0
c06361 0510 2825 ▲ 239 15.8 51 1000 0
c01aae 0134 3600 ▼ 169 18.9 227 4917 0
c0227b REN05 2045 4750 253 20.2 47 803 2
ad2445 JBU633 1326 32000 427 29.8 278 3457 0
a27d9b N26KK 1200 3800 ▼ 179 31.0 78 1510 1
c0796c CGTZN 0176 850 ▲ 72 36.0 9 420 10
c0796e CGTZP 0174 2725 ▼ 122 36.7 305 422 4
a4fc92 2600 90 38.0 103 406 4
a6a711 3543 32000 441 41.9 270 1374 2
c02e94 SKV7606 0554 22300 ▲ 401 42.7 113 2733 19
c07f05 WJA1211 6607 19750 ▼ 324 43.5 310 530 0
c06262 POE139 2240 17300 ▲ 306 43.7 107 4015 27
c019c3 CFJTQ 4310 3750 136 46.7 161 413 0
a61584 3750 270 48.0 317 332 0
a7b92b UAL351 7056 36000 434 52.0 269 165 12
a37023 DAL2549 7045 35000 480 53.0 104 4114 1
c07d20 6310 20275 ▲ 319 54.0 64 7312 0
c06b0b 0664 15700 207 56.7 252 3066 0
aadd37 N8AM 5723 25125 295 60.1 98 1633 0
ac386d 4104 10750 ▼ 419 62.5 16 624 0
a22003 ENY3355 5663 11625 ▼ 391 62.9 53 237 0
Lake Superior
Saguenay
Québec
Sudbury
Sault Ste. Marie
Trois-Rivières
Drummondville
Ottawa
Montréal
Sherbrooke
Lake Huron
Green Bay
Barrie
Peterborough
Kingston
Vermont
New Hampshire
Milwaukee
Grand Rapids
Sarnia
Syracuse
New York
Manchester
Kenosha
Lansing
Flint
London
Albany
Lowell
Detroit
Chatham
Erie
Massachusetts
Kalamazoo
Ann Arbor
Springfield
Providence
Chicago
South Bend
Toledo
Cleveland
Connecticut
Fall River
Gary
Scranton
Bridgeport
Fort Wayne
Akron
Pennsylvania
Islip
Allentown
New York
Pittsburgh
Harrisburg
Reading
Trenton
Indiana
Dayton
Columbus
Wilmington
New Jersey
Ohio
Maryland
Cincinnati
Washington
West Virginia
Louisville
Lexington
Charleston
Evansville
Kentucky
Virginia
Richmond
Roanoke
Virginia Beach
Nashville
Greensboro
Raleigh
© OpenStreetMap contributors.

„IoT” (ale zwykle bez I)

Różne urządzenia radiowe w paśmie ISM (zwykle 433MHz)

- Stacje pogodowe itp.
- Tanie piloty (lepsze mają zmienny kod)
- Liczniki energii, liczniki wody (czy sąsiedzi wyjechali na urlop?)
- Dzwonki (a potem replay attack :)

  https://github.com/merbanan/rtl_433

Grubszy kaliber:

- Protokół STQC (syreny strażackie, powiadamianie ludności). Sekwencja tonów, brak autoryzacji:

  https://github.com/sq5bpf/multimon-ng-stqc
- Radiostop. Awaryjne zatrzymywanie pociągów za pomocą sekwencji 3 tonów. Radio to nie tylko niewinna zabawa.

Służby i łączność komercyjna

- Pozwolenia dla firm wydaje UKE i publikuje je a swojej stronie, wyszukiwarka: http://kosu77.ugu.pl
- Istnieje nieoficjalny podział częstotliwości dla służb:

  https://web.archive.org/web/20130103164830/http://giller.pl/radioscanner/strony/gdzie.html
- Oprogramowanie do słuchania radiotelefonów cyfrowych:

  DMR (m.in. policja), NXDN, P25: https://github.com/szechyjs/dsd

  TETRA (np. metro, lotnisko, policja): https://github.com/sq5bpf/telive

  MPT1327 (np. energetyka): https://github.com/DSheirer/sdrtrunk

  i wiele innych...
- Czasem nie cały ruch jest szyfrowany (względy ekonomiczne: dodatkowy koszt licencji, problemy z dystrybucja kluczy do szyfrowania, bugi w konfiguracji).

Służby i łączność komercyjna

- Inmarsat (głos, pagery, dane przez satelitę) http://www.inmarsatdecoder.com/ (niestety płatne oprogramowanie)
- Iridium (głos, pagery, dane przez satelitę) https://github.com/muccc/iridium-toolkit
- DVB (TV i dane przez satelitę) w tym downlink danych via satelita http://dvbsnoop.sourceforge.net/

  Ciężka do wyśledzenia komunikacja (np. do C&C) via satelita:

  Wysyłanie pakietów: IP Spoofing, odbieranie: downlink z satelity
- https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/09/20081827/BlackHat-DC-2010-Nve-Playing-with-SAT-1.2-wp.pdf
- Turla APT:

  https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/

Piraci :)

- Każdy system łączności ma swoich „nieautoryzowanych użytkowników”
- Radio pirackie, lokalnie w paśmie UKF, nielokalnie na falach średnich i krótkich, szczególnie w weekendy. http://alfalima.net/
- Echo-Charlie: okolice 6.660MHz LSB, obecnie rzadkie. Holandia, Włosi itp
- Łączność Rosjan w okolicy 3MHz AM (диапазон свабодных радистов)

  Wiele satelit retransmituje (bez analizy) to co dostały ze stacji naziemnych
- Satelity geostacjonarne NATO „Satcom” https://uhf-satcom.com/

  240-300MHz (w tym stare wojskowe satelity NATO)

  Częstotliwość wejściowa często 41MHz wyżej (jakby ktoś pytał :)

  255.550 MHz – częstotliwość uwielbiana przez brazylijskich piratów.

  Nie tylko Ameryka Południowa, satcomów używają też często Rosjanie.

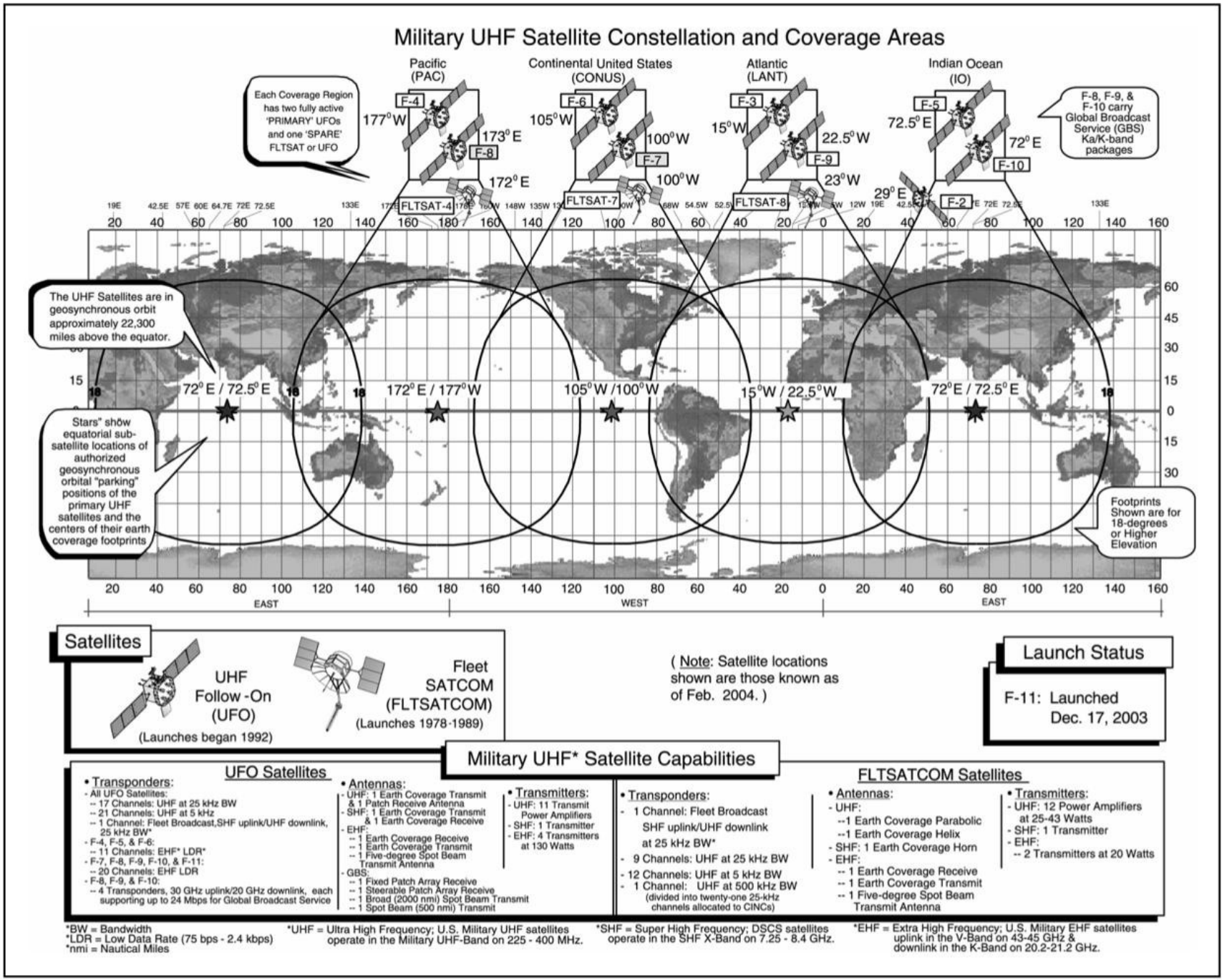


Figure I-6. Military UHF Satellite Constellation and Coverage Areas

Nadawanie

Należy nadawać tylko na częstotliwościach na które ma się pozwolenie (np. krótkofalarskie). Odradzam piracenie, dlatego o tym jest tylko jeden slajd :)

- Radiotelefony VHF/UHF. Np Baofeng UV-5R 137-174 MHz i 400-470 MHz, 5W, modulacja FM
- Osmo-fl2k (tania przejściówka USB 3.0 na VGA). Jest to 3-kanałowy przetwornik CA z samplowaniem do 150MHz https://osmocom.org/projects/osmo-fl2k/wiki
- RPItx (nadawanie z raspberry pi za pomoca wbudowanego PWM-a): https://github.com/F5OEO/rpitx

- SDR z możliwością nadawania:

  HackRF

  ADALM PLUTO-SDR

  USRP

  … i wiele innych
- Własne konstrukcje. Np gotowy moduł nadajnika IoT na 433MHz (koszt rzędu 10zł) i Rpi albo arduino

Linki

- https://www.rtl-sdr.com/
- https://forums.radioreference.com/
- Czasem http://radioscanner.pl/
- Czasem https://www.elektroda.pl/rtvforum/forums.html
- Informajce publikowane na facebooku (zwykle średniej jakości, nie polecam)
- http://www.websdr.org/ (odbiorniki dostępne przez internet)
- http://osmocom.org/projects
- https://pzk.org.pl/ Polski Związek Krótkofalowców
- https://github.com/jopohl/urh

Bądźmy (radio) amatorami

takimi którzy nie wiedzą że czegoś się nie da zrobić

(więc to robią :)

PYTANIA?

VY 73

Jacek Lipkowski SQ5BPF
SQ5BPF@lipkowski.org

Link do prezentacji:

https://github.com/sq5bpf/misc/blob/master/wth2019.pdf