Zabawa z radiami zdefiniowanymi programowo

Wprowadzenie

Termin radio zdefiniowane programowo oznacza implementację sprzętowych komponentów radiowych, takich jak modulatory, demodulatory i tunery, przy użyciu oprogramowania. W tym rozdziale omówimy różne przepisy i przyjrzymy się wielu sposobom, w jaki RTLSDR może być używany do zabawy z częstotliwościami i danymi przesyłanymi przez nie.

Skanery częstotliwości radiowych

RTLSDR to bardzo tanie (około 20 USD) radio zdefiniowane programowo, które wykorzystuje klucz sprzętowy tunera telewizji DVB-T. W tym przepisie omówimy podłączanie urządzenia RTLSDR z Kali Linux, aby sprawdzić, czy zostało pomyślnie wykryte.

Przygotowania

Będziemy potrzebować sprzętu do tego przepisu. Można go łatwo kupić na Amazon lub na stronie https:/ / www. rtl- sdr. com/ buy- rtl- sdr- dvb- t- dongles/ . Kali ma już narzędzia, dzięki którym możemy zacząć z nim pracować.

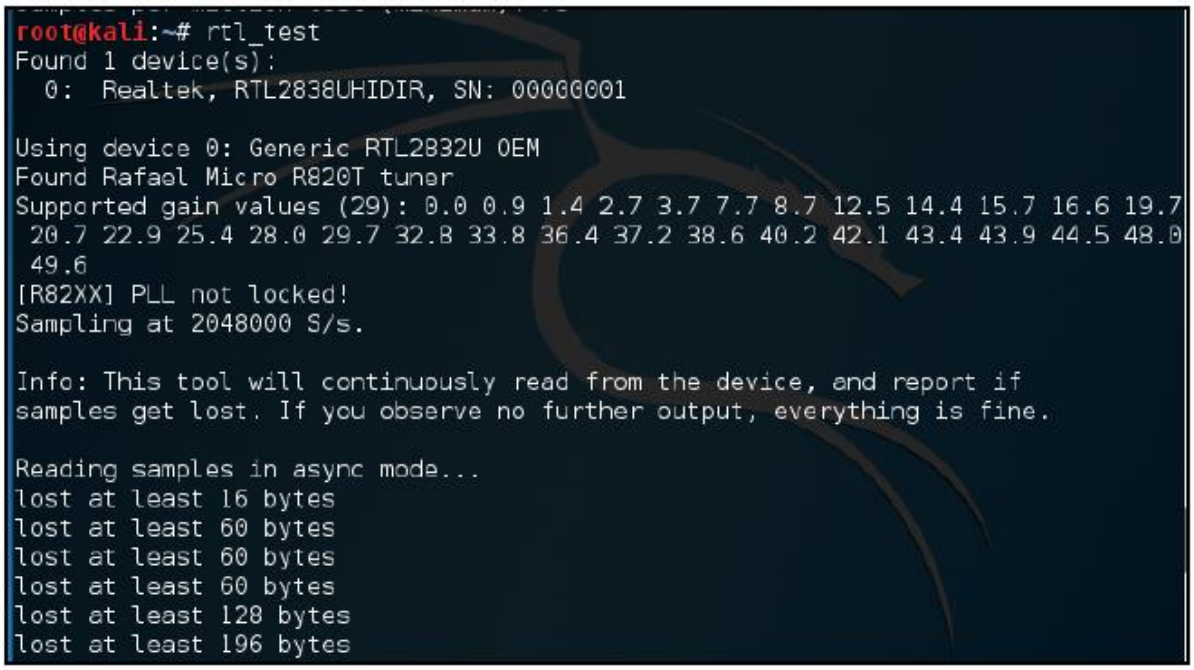
Jak to zrobić...

Podłączamy nasze urządzenie i powinno zostać wykryte w Kali Linux. Urządzenia często zachowują się nieprawidłowo. Oto przepis na uruchomienie testu:

1. Najpierw uruchomimy test za pomocą polecenia:

rtl_test

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:



2. Możemy zobaczyć kilka upuszczonych pakietów. Dzieje się tak, ponieważ próbowaliśmy tego w konfiguracji VM z samym USB 2.0.

3. W przypadku dużej liczby utraconych pakietów możemy to sprawdzić, ustawiając niższą częstotliwość próbkowania za pomocą rtl_test -s 10000000:

4. Teraz jesteśmy gotowi przejść do następnego przepisu i pobawić się naszym urządzeniem.

Praktyczna praca ze skanerem RTLSDR

Skaner RTLSDR to wieloplatformowy interfejs graficzny, którego można używać do analizy widma. Skanuje on dany zakres częstotliwości i wyświetla wynik w postaci spektrogramu.

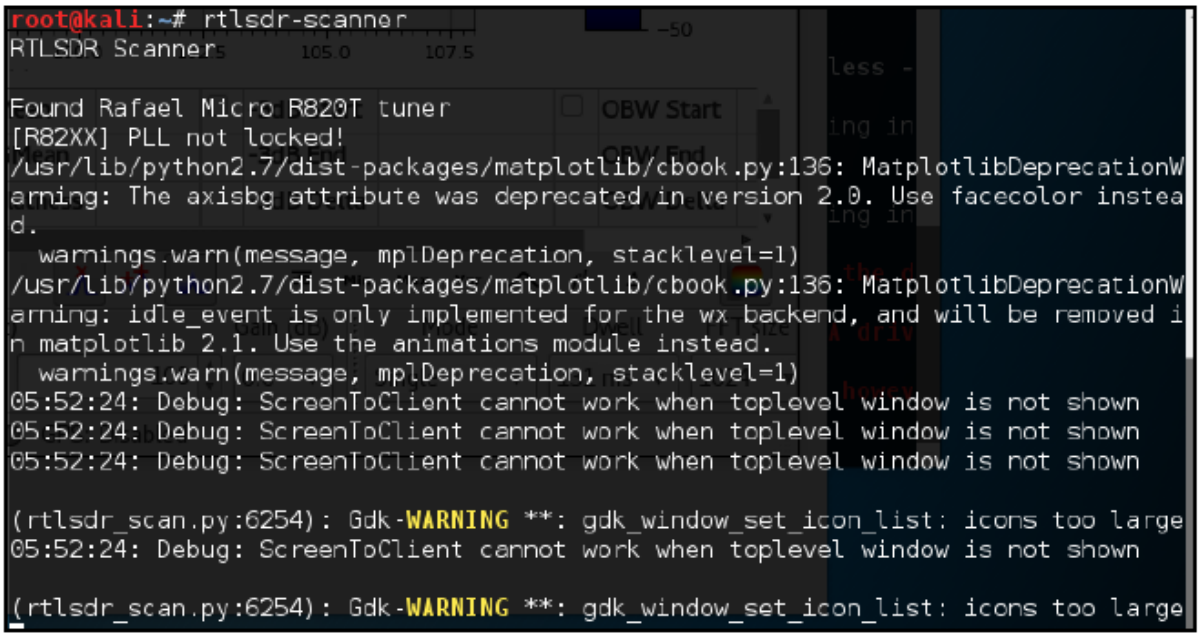
Jak to zrobić...

Oto przepis na uruchomienie rtlsdr-scanner:

1. Podłączamy RTLSDR do systemu i uruchamiamy skaner za pomocą polecenia:

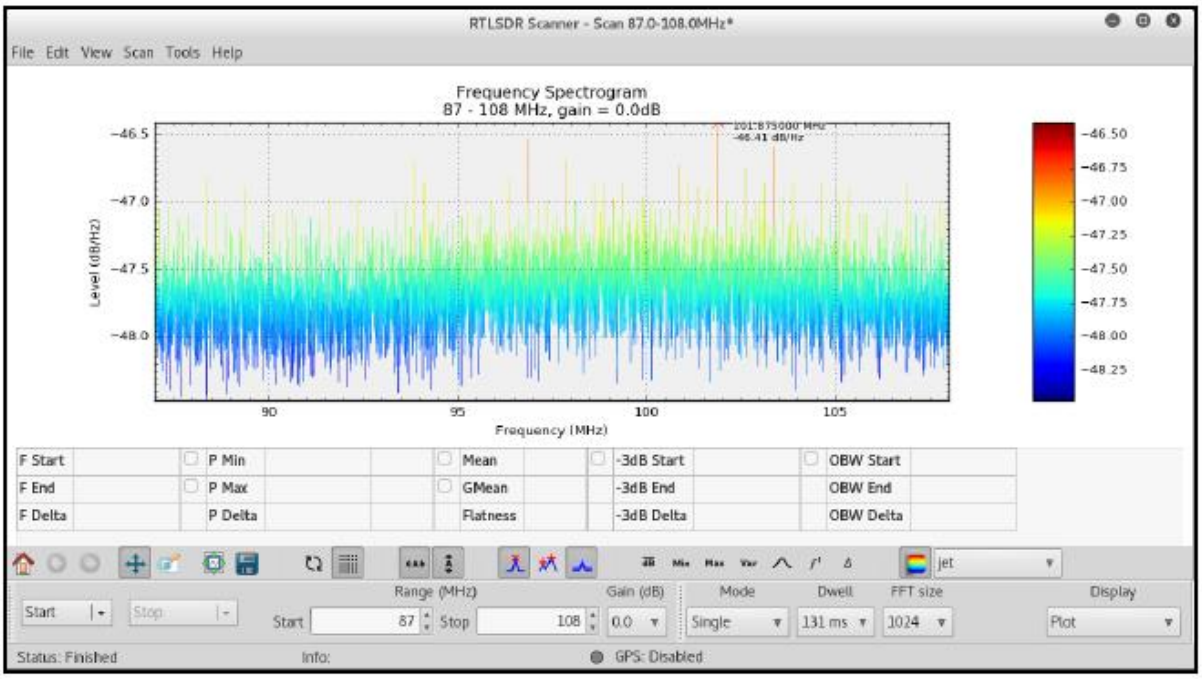
rtlsdr-scanner

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:



2. Powinno otworzyć się nowe okno pokazujące interfejs graficzny narzędzia; w tym miejscu wystarczy wpisać zakres częstotliwości, w którym chcemy przeprowadzić skanowanie, i kliknąć Rozpocznij skanowanie:

3. Zajmie trochę czasu, zanim zobaczymy przegląd częstotliwości, a następnie zobaczymy wynik w formacie graficznym:



Jeśli aplikacja przestanie odpowiadać, zaleca się obniżenie

zakresu i wybranie Single jako Mode zamiast continuous.

Zabawa z gqrx

Narzędzie gqrx to odbiornik radiowy (SDR) typu open source, oparty na radiu GNU i graficznym zestawie narzędzi Qt. Posiada wiele funkcji, takich jak:

* Wykrywanie urządzeń podłączonych do komputera

* Przetwarzanie danych I/Q

* Demodulatory AM, SSB, CW, FM-N i FM-W (mono i stereo)

* Nagrywanie i odtwarzanie dźwięku do/z pliku WAV

* Nagrywanie i odtwarzanie surowych danych pasma podstawowego

* Przesyłanie strumieniowe dźwięku przez UDP

W tym przepisie omówimy podstawy gqrx i innego narzędzia, RTLSDR

Jak to zrobić...

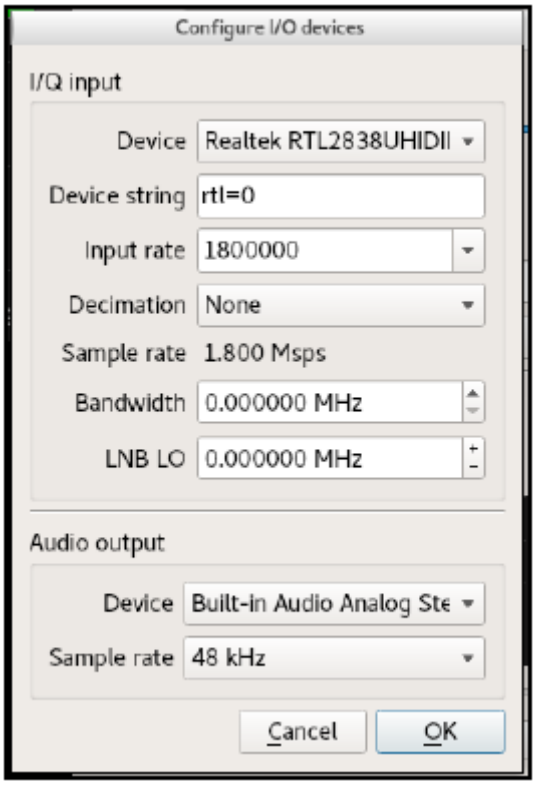
Oto przepis na użycie gqrx:

1. Możemy zainstalować gqrx za pomocą polecenia:

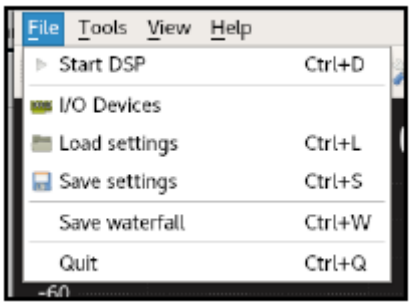
apt install gqrx

2. Po wykonaniu tej czynności uruchamiamy narzędzie, wpisując gqrx.

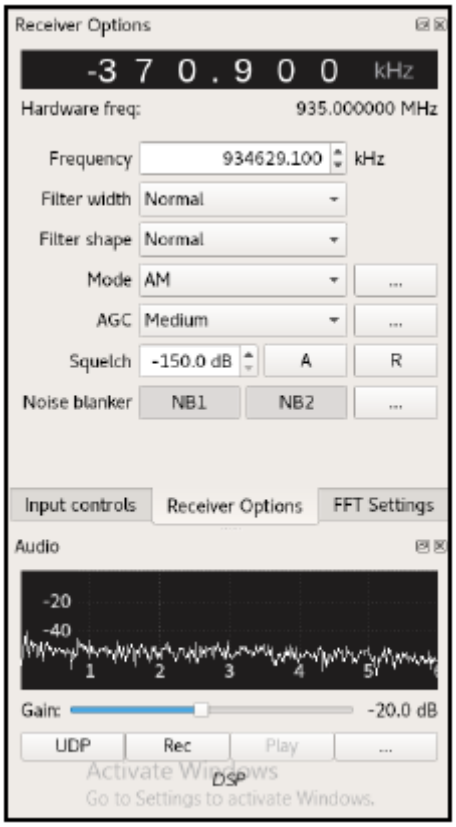
3. Wybieramy nasze urządzenie z menu rozwijanego w oknie, które się otworzy i klikamy OK:.



4. Teraz otwiera się aplikacja GQRX, a po prawej stronie w oknie odbiornika wybieramy częstotliwość, którą chcemy wyświetlić. Następnie przechodzimy do pliku i klikamy na Start DSP:

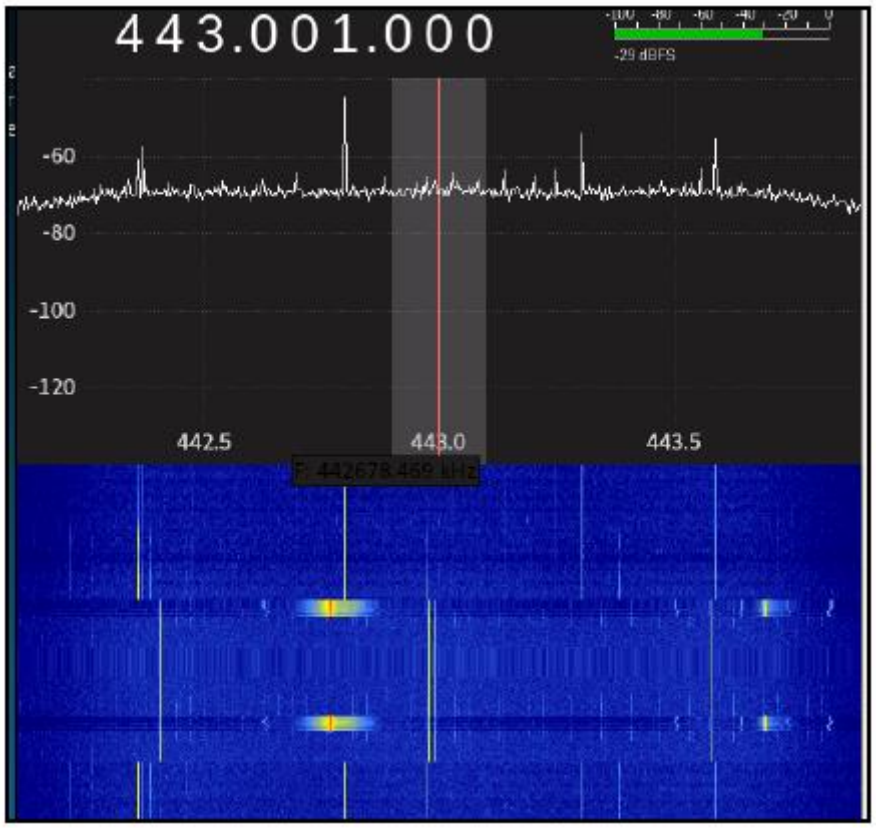


5. Teraz widzimy wodospad i powinniśmy zacząć słyszeć dźwięk w naszym głośniku. Możemy nawet zmienić częstotliwość, której słuchamy, używając przycisków w górę i w dół w oknie Opcje odbiornika:



6. Przyjrzymy się przykładowi pilota samochodowego, który służy do zamykania/otwierania samochodu.

7. Po kilkukrotnym naciśnięciu przycisku zobaczymy zmianę w wodospadzie pokazującą różnicę w sygnale:

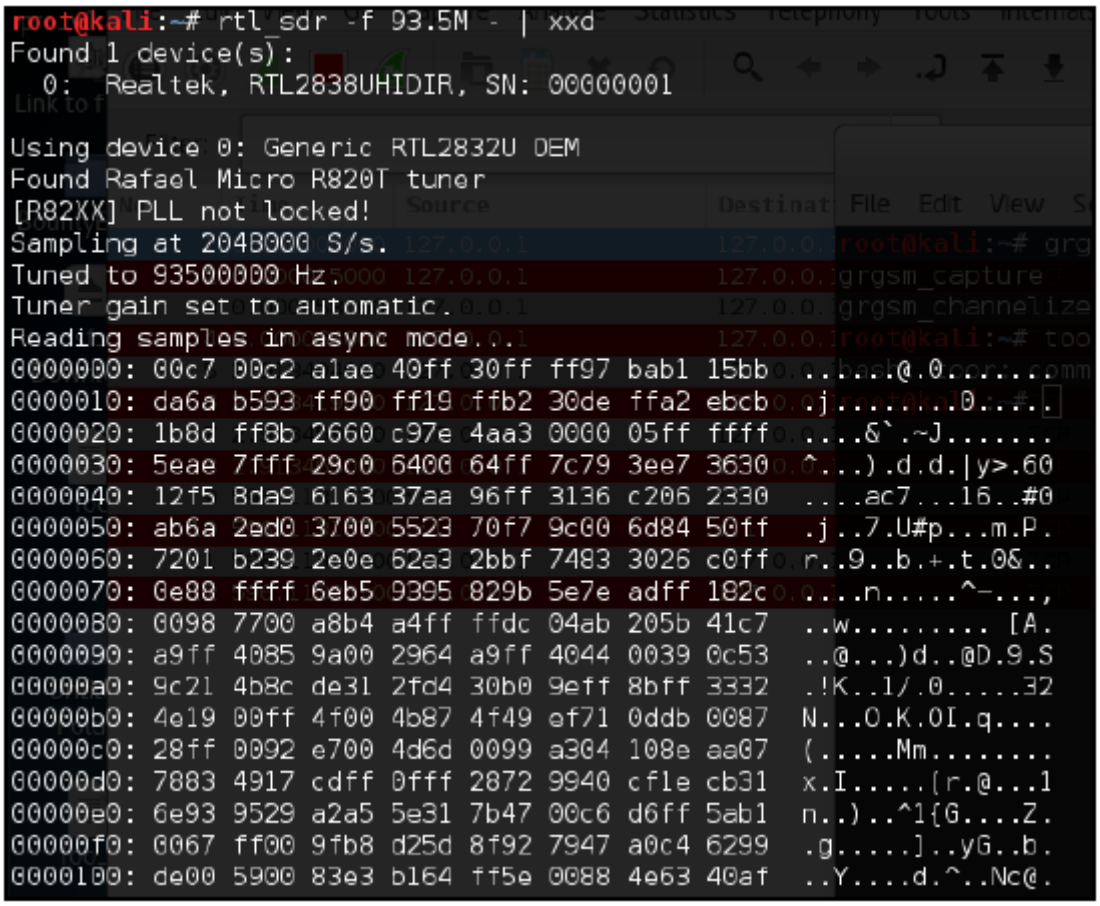


8. Możemy nagrać sygnał w oknie nagrywania, a następnie go zapisać. Później można go zdekodować i przesłać z powrotem do samochodu za pomocą transpondera, aby go odblokować.

9. Aby przechwycić dane przy częstotliwości 443 MHz, możemy użyć polecenia:

rtl_sdr -f 443M - | xxd

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:



Urządzenie kalibrujące do podsłuchu GSM

RTLSDR pozwala nam również przeglądać ruch GSM za pomocą narzędzia o nazwie kal lub kalibrate-rtl. To narzędzie może skanować stacje bazowe GSM w paśmie częstotliwości. W tym przepisie nauczymy się korzystać z kalibrate, a następnie potwierdzimy kanał w gqrx.

Jak to zrobić...

Oto kroki korzystania z kalibrate:

1. Większość krajów korzysta z pasma GSM900. W USA jest to 850. Użyjemy następującego polecenia, aby przeskanować stacje bazowe GSM:

kal -s GSM900 -g 40

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

```
root@kali:~/.config# kal -s GSM900  -g 40
Found 1 device(s):
  0:  Generic RTL2832U OEM

Using device 0: Generic RTL2832U OEM
Detached kernel driver
Found Rafael Micro R820T tuner
Exact sample rate is: 270833.002142 Hz
[R82XX] PLL not locked!
Setting gain: 40.0 dB
kal: Scanning for GSM-900 base stations.
```

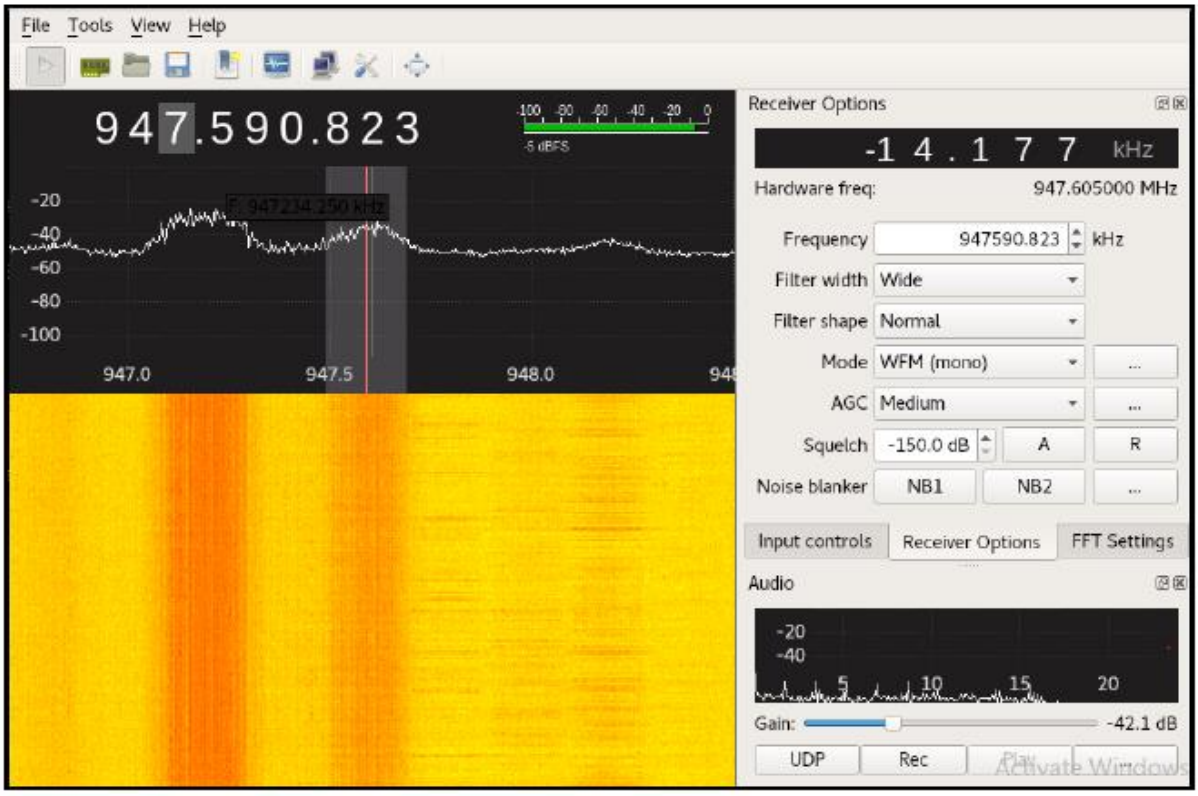
2. Za kilka minut wyświetli nam się lista stacji bazowych:

```
GSM-900:


        chan: 32 (941.4MHz - 15.209kHz) power: 991758.24
        chan: 34 (941.8MHz - 15.099kHz) power: 835333.49
        chan: 51 (945.2MHz - 14.653kHz) power: 2857467.65
        chan: 53 (945.6MHz - 14.620kHz) power: 3310824.09
        chan: 57 (946.4MHz - 15.736kHz) power: 2261161.19
        chan: 61 (947.2MHz - 15.201kHz) power: 4090351.91
        chan: 63 (947.6MHz - 14.177kHz) power: 2990914.87
```

3. Zapisujemy częstotliwość; w naszym przypadku użyjemy 947,6 MHz wraz z przesunięciem.

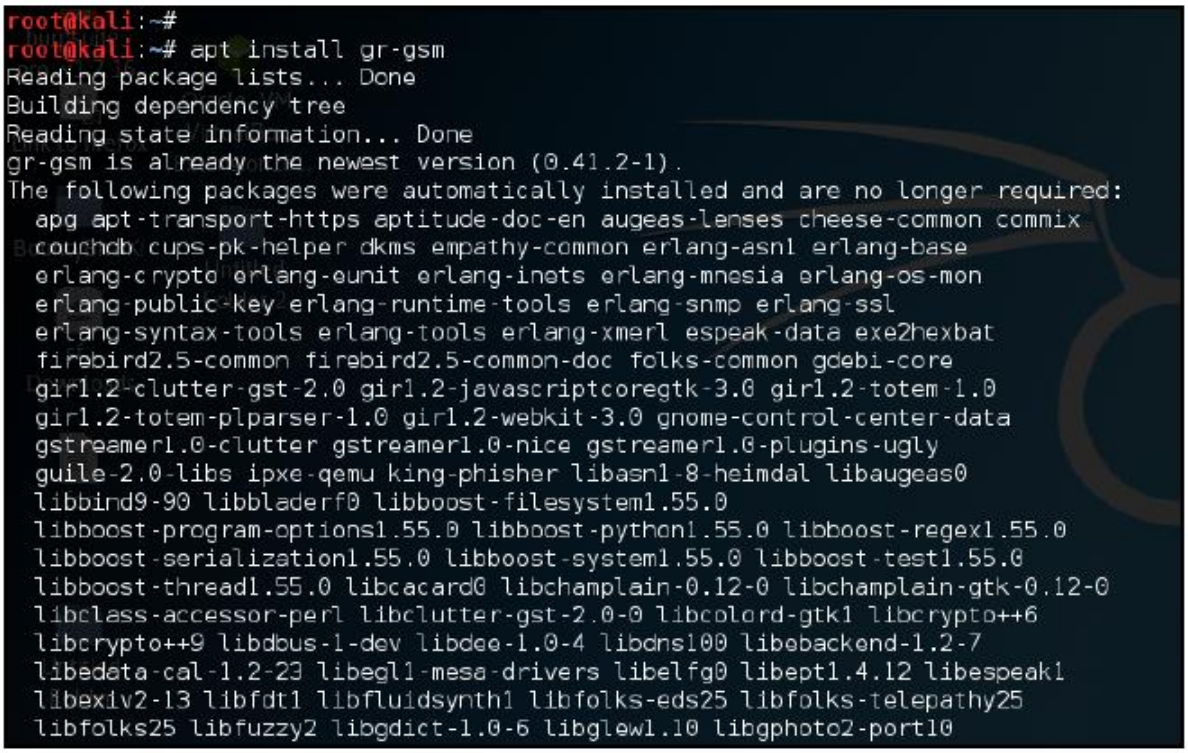
4. Teraz otwieramy GQRX i wprowadzamy go w oknie Opcje odbiornika:



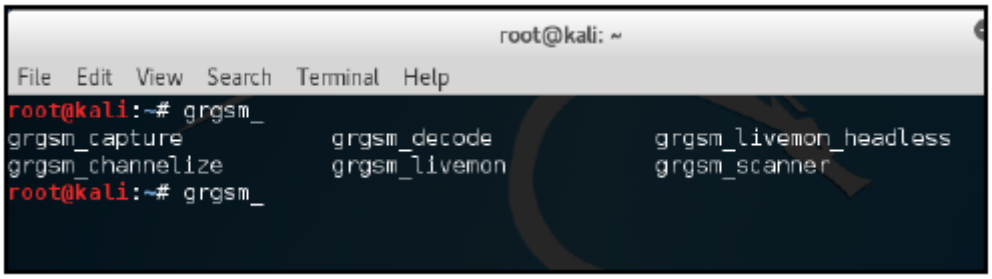
5. Na wykresie wodospadu widać, że urządzenie doskonale wychwytuje sygnały.

6. Teraz przyjrzymy się tym danym na poziomie pakietów. Użyjemy narzędzia znanego jako grgsm.

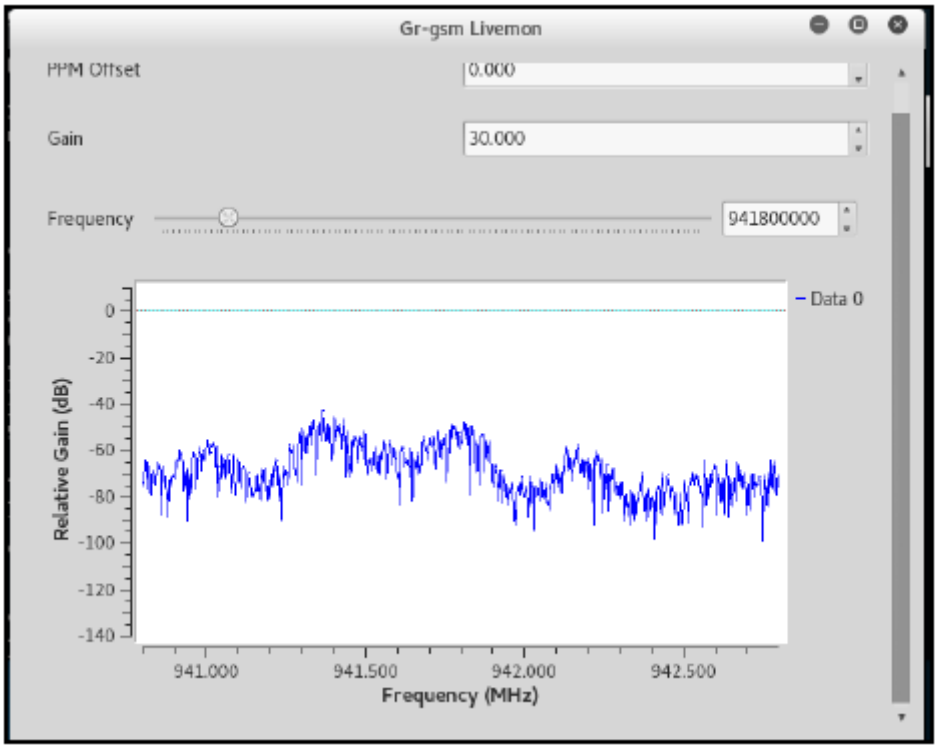
7. Można je zainstalować za pomocą apt install gr-gsm:



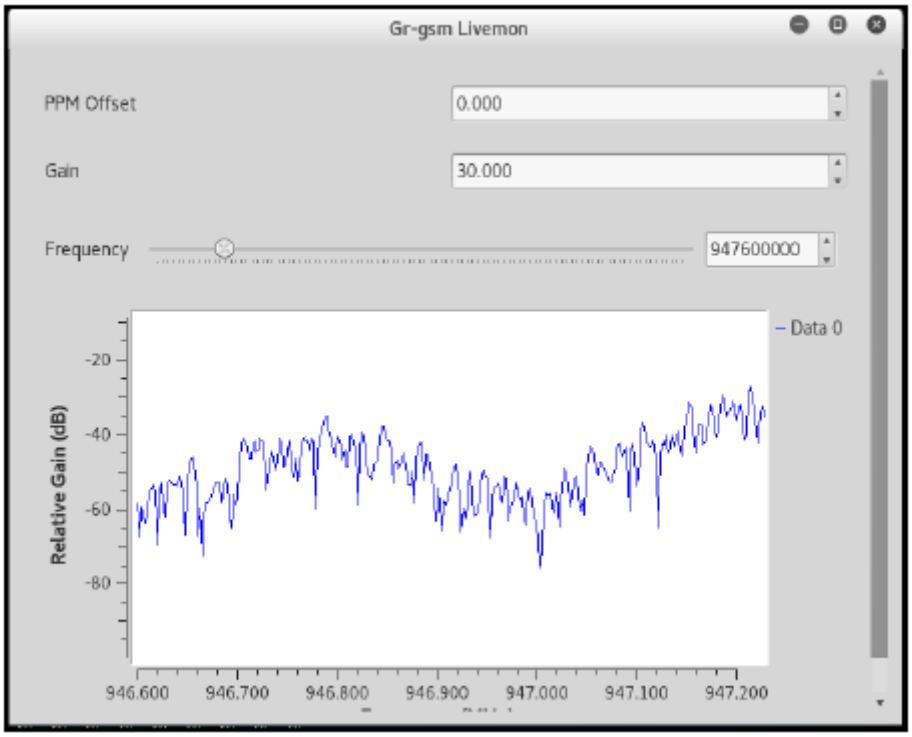
8. Po wykonaniu tej czynności, jeśli wpiszemy grgsm_ i naciśniemy klawisz Tab, wyświetli się nam lista różnych dostępnych narzędzi:



9. Najpierw użyjemy grgsm_livemon do monitorowania pakietów GSM na żywo. Otworzymy terminal i wpiszemy grgsm_livemon:



10. W nowym oknie, które się otworzy, przełączymy się na częstotliwość, którą przechwyciliśmy w poprzednich krokach za pomocą kalibrate:

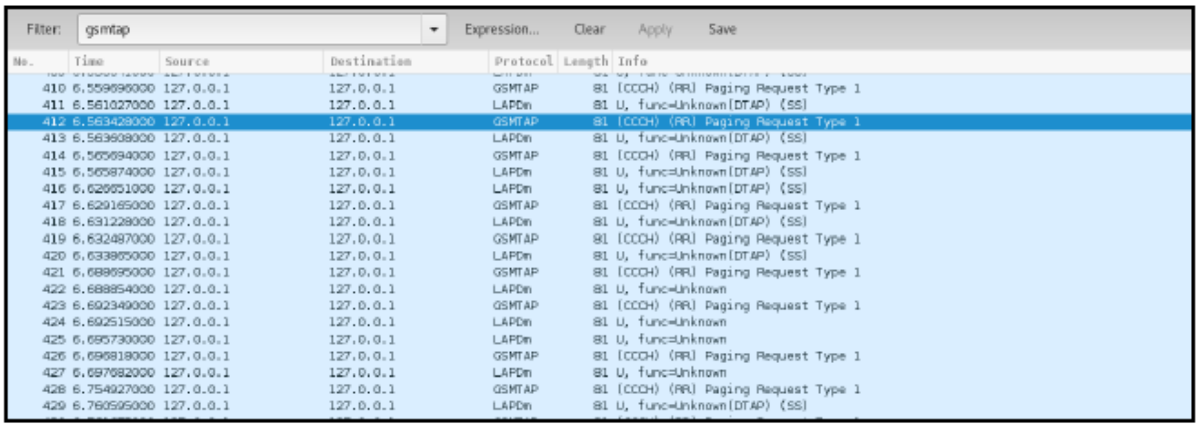


11. Możemy powiększyć określony zakres, przeciągając i zaznaczając obszar w oknie graficznym.

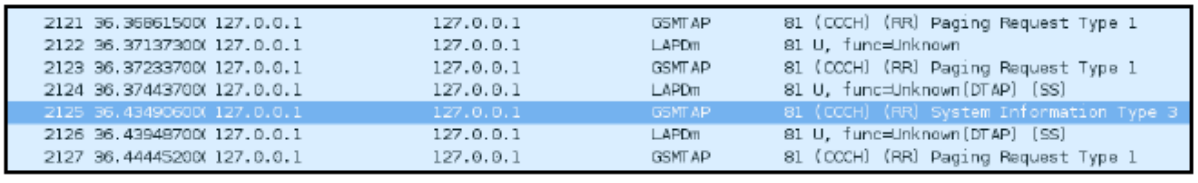
12. W nowym oknie terminala uruchamiamy Wireshark, wpisując wireshark.

13. Następnie ustawiamy adapter na Loopback: lo i rozpoczynamy przechwytywanie pakietów:

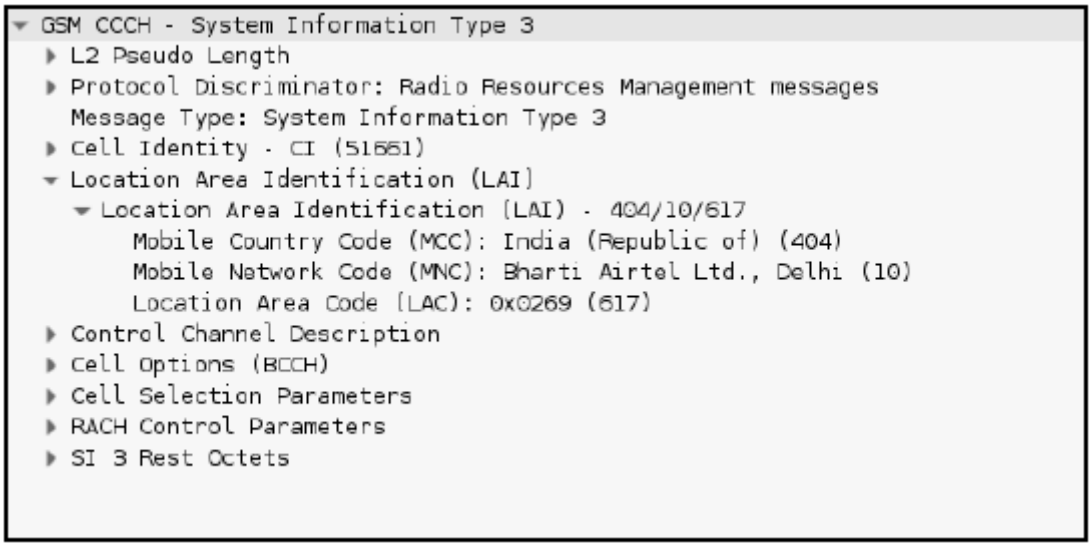
14. Następnie dodajemy filtr gsmtap:



15. Powinniśmy zobaczyć pakiety w oknie informacyjnym. Powinniśmy zobaczyć pakiet z etykietąSystem Information Type 3; otwórzmy go:



16. Zobaczymy informacje systemowe, takie jak kod kraju telefonu komórkowego, kod sieci i kod obszarowy lokalizacji:



17. Dzięki temu przepisowi dowiedzieliśmy się, jak przesyłane są pakiety GSM.

Dekodowanie wiadomości ADS-B za pomocą Dump1090

ADS-B oznacza Automatic Dependent Surveillance-Broadcast (automatyczny zależny nadzór-rozgłaszanie). Jest to system, w którym sprzęt elektroniczny na pokładzie samolotu automatycznie nadaje dokładną lokalizację samolotu za pośrednictwem cyfrowego łącza danych. Jak opisano w oficjalnym pliku readme narzędzia, Dump1090 to dekoder Mode S zaprojektowany specjalnie dla urządzeń RTLSDR. Główne cechy to:

* Solidne dekodowanie słabych wiadomości. Dzięki mode1090 wielu użytkowników zauważyło lepszy zasięg w porównaniu z innymi popularnymi dekoderami.

* Obsługa sieci — strumień TCP30003 (MSG5), surowe pakiety, HTTP.

* Wbudowany serwer HTTP, który wyświetla aktualnie wykryte samoloty na Mapach Google.

* Jednobitowa korekcja błędów przy użyciu 24-bitowego CRC.

* Możliwość dekodowania wiadomości DF11 i DF17.

* Możliwość dekodowania formatów DF, takich jak DF0, DF4, DF5, DF16, DF20 i DF21, gdzie suma kontrolna jest XOR-owana z adresem ICAO poprzez brutalne wymuszenie pola sumy kontrolnej przy użyciu adresów ICAO, które omówiliśmy.

* Dekodowanie surowych próbek IQ z pliku (za pomocą przełącznika wiersza poleceń --ifile).

* Interaktywny tryb CLI, w którym aktualnie wykryte samoloty są wyświetlane jako lista, odświeżana w miarę napływania nowych danych.

* Dekodowanie współrzędnych CPR i obliczanie śladu na podstawie prędkości.

* Serwer TCP przesyła strumieniowo i odbiera surowe dane do/od podłączonych klientów (za pomocą --net).

W tym przepisie użyjemy tego narzędzia do przeglądania ruchu lotniczego za pomocą wizualizacji.

Jak to zrobić...

Oto kroki, aby użyć Dump1090:

1. Możemy pobrać narzędzie z repozytorium Git, używając polecenia git clone https://github.com/antirez/dump1090.git:

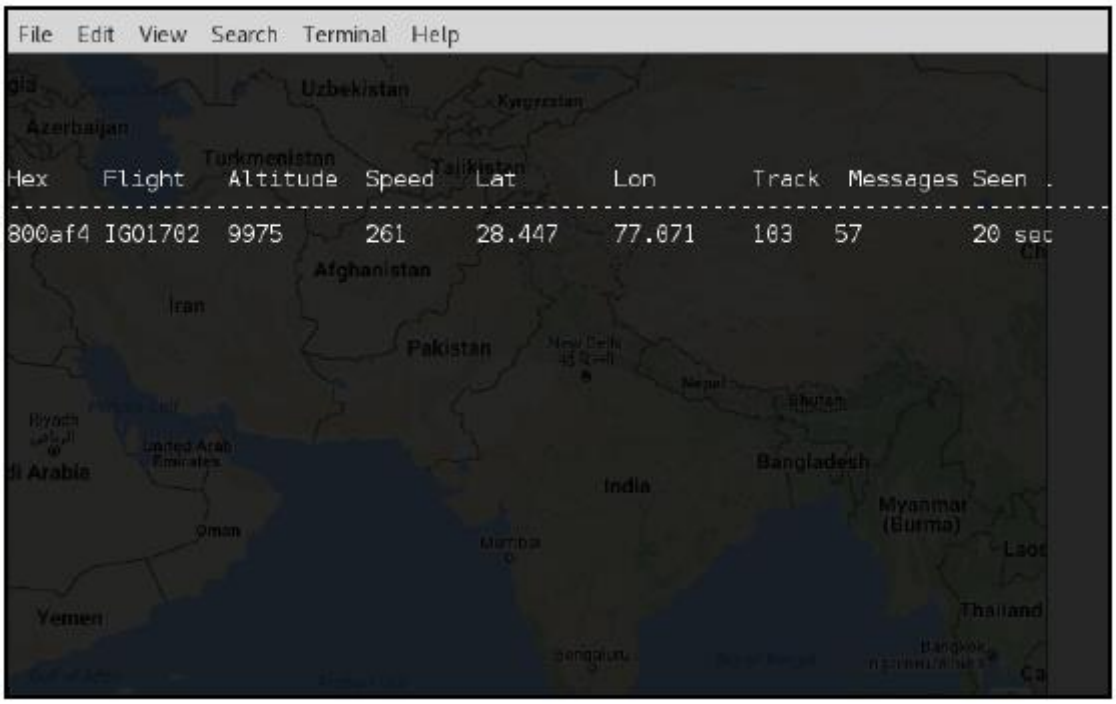
```
root@kali:~# git clone https://github.com/antirez/dump1090.git
Cloning into 'dump1090'...
remote: Counting objects: 265, done.
remote: Total 265 (delta 0), reused 0 (delta 0), pack-reused 265
Receiving objects: 100% (265/265), 536.32 KiB | 266.00 KiB/s, done.
Resolving deltas: 100% (147/147), done.
root@kali:~#
```

2. Po pobraniu przechodzimy do folderu i uruchamiamy make.

3. Teraz powinniśmy mieć plik wykonywalny. Możemy uruchomić narzędzie za pomocą następującego polecenia:

./dump1090 --interactive -net

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:



4. Za kilka minut powinniśmy zobaczyć loty, a po otwarciu przeglądarki na http://localhost:8080 będziemy mogli zobaczyć loty również na mapie.