TRZYDZIESTE FORUM TELEINFORMATYKI®

Bezzałogowy System Powietrzny Rozpoznania i Ataku Sieci Radiowych HackBee

Autorzy projektu:

por. mgr inż. Rafał SZCZEPANIK por. mgr inż. Tomasz WALCZYNA

Doktoranci Szkoły Doktorskiej Wojskowej Akademii Technicznej

PLAN PREZENTACJI

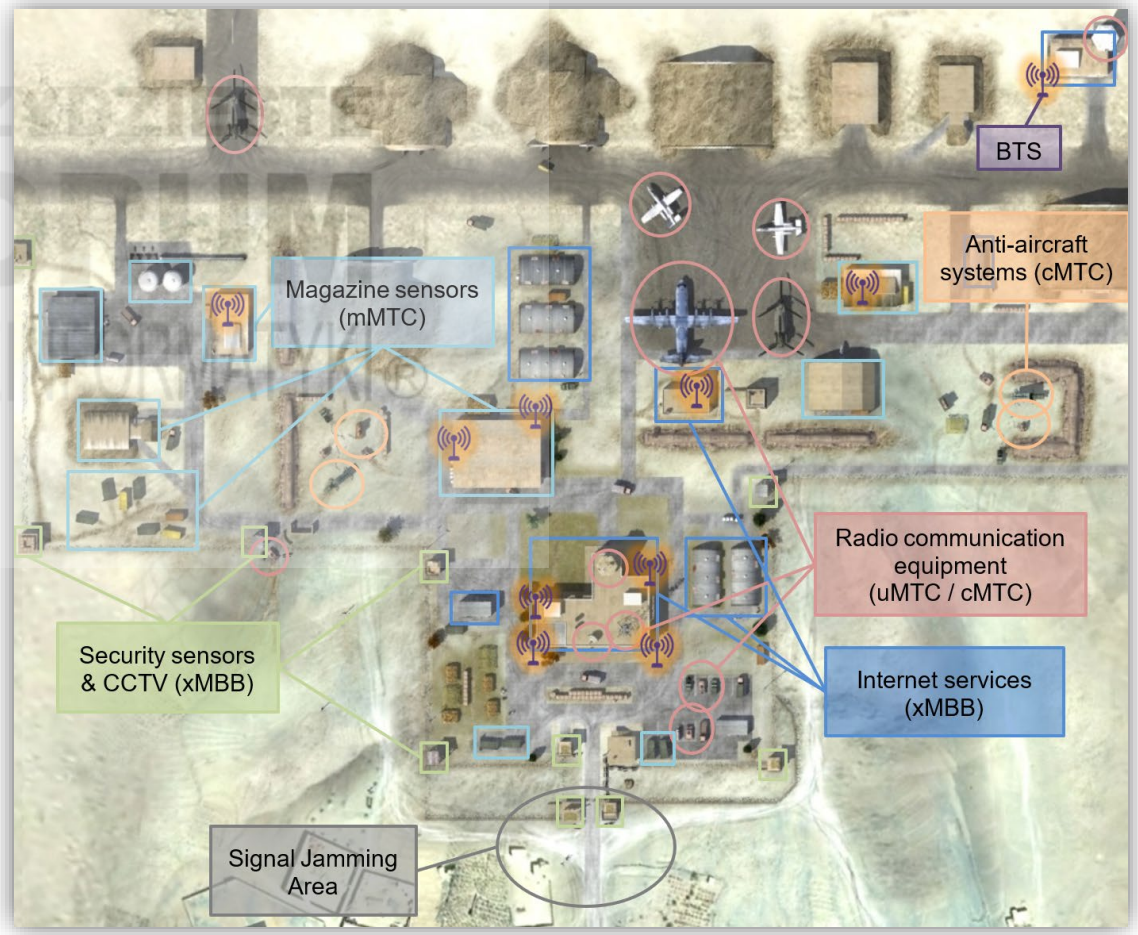
- **Koncepcja BSP,**
- **Budowa BSP,**
- **Przygotowanie UAV i systemu operacyjnego,**
- **Ataki na radiowe sieci Wi-Fi,**
- **Mobilne sieci telefonii komórkowej,**
- **Zakłócanie GPS,**
- **Hackowanie dronów komercyjnych,**
- **Rozpoznanie radiowe,**
- **Zastosowanie w obszarze obronności RP.**

Koncepcja opracowanego BSP

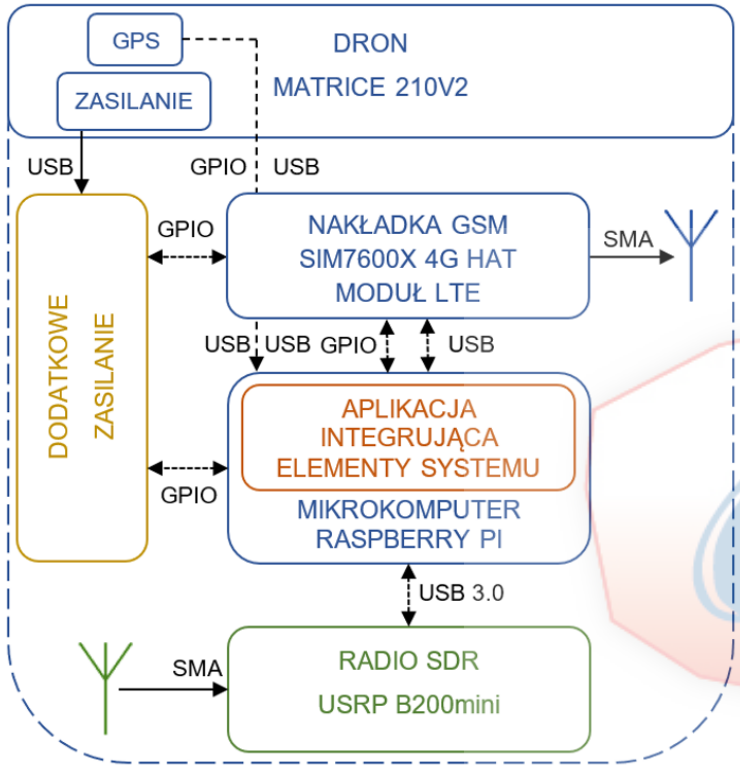
Celem projektu było opracowanie Bezzałogowego Systemu Powietrznego **HackBee** pozwalającego na rozpoznanie sieci radiowych tj. urządzeń telefonii komórkowych, radiowych sieci teleinformatycznych oraz demonstrację technologii pozwalającej na przeprowadzanie mobilnych ataków cybernetycznych.

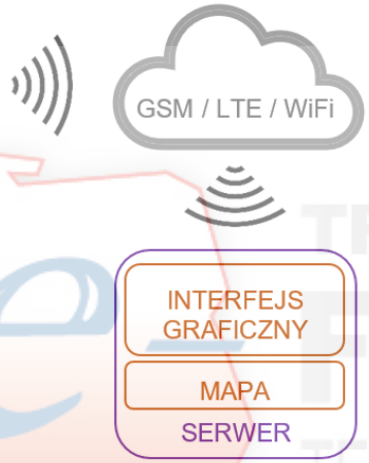
Głównym **zadaniem systemu** jest:

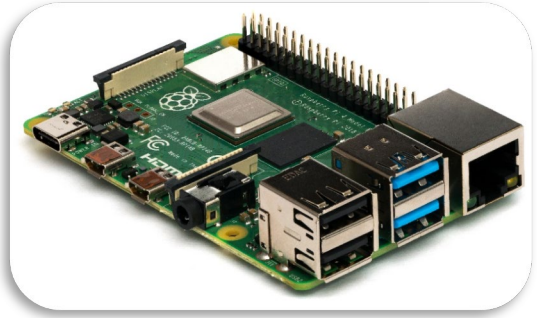
- wykrycie oraz sniffing radiowych sieci bezprzewodowych;
- możliwość przeprowadzenia ataków penetracyjnych sieci radiowych;
- monitorowanie widma elektromagnetycznego;
- zakłócanie systemów GPS;
- wykrycie oraz rozpoznanie na poziomie taktycznym urządzeń telefonii komórkowej;
- tworzenie radiowych punktów dostępowych – własnej sieci komórkowej.

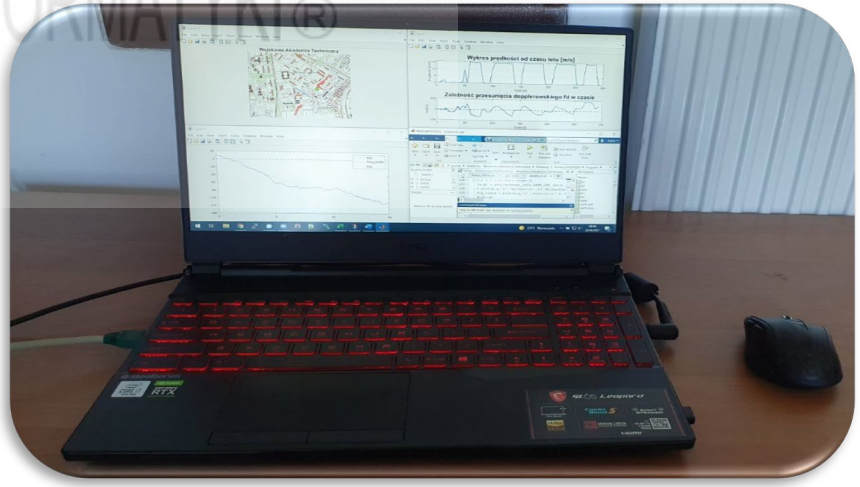


Budowa BSP HackBee









Ataki na sieci Wi-Fi mogą przybierać różne formy, od klasycznych prób przejęcia hasła dostępowego, po bardziej zaawansowane taktyki, takie jak man-in-the-middle czy ataki słownikowe.

W zbudowanym systemie wykorzystano różnorodne metody i narzędzia do atakowania radiowych sieci Wi-Fi.

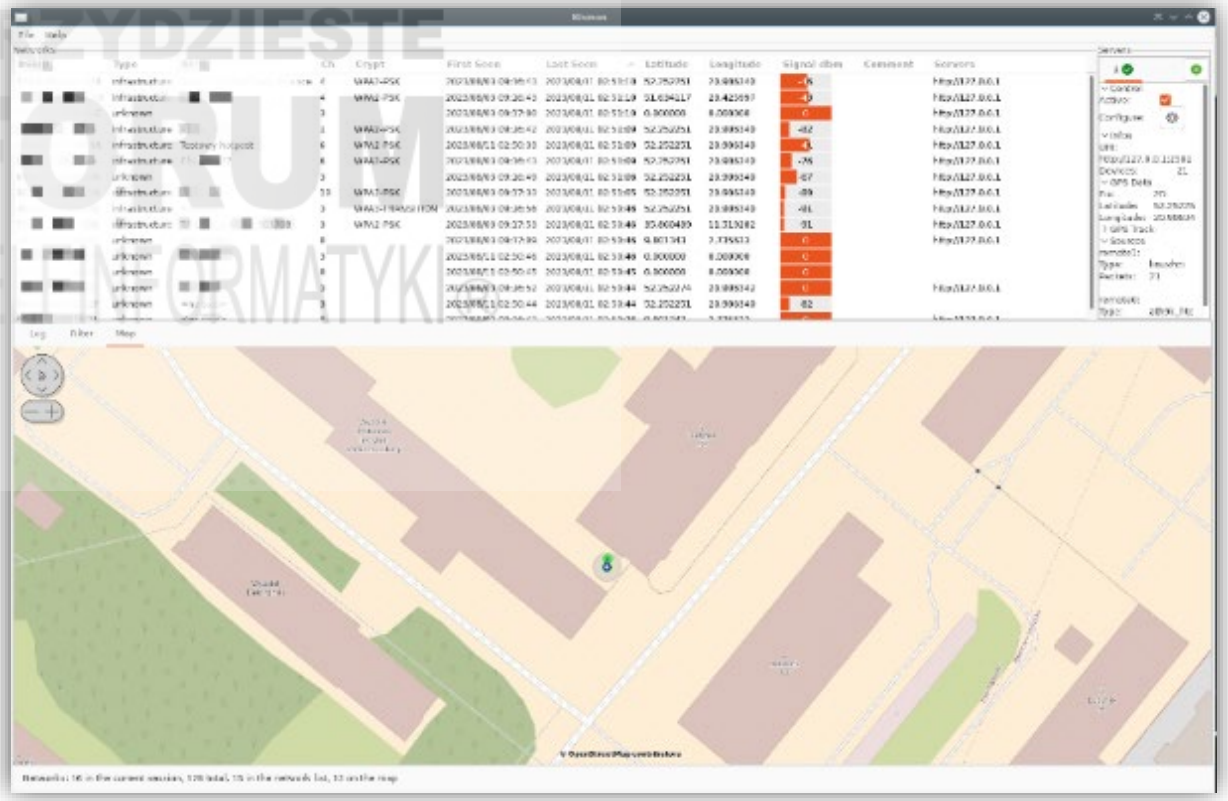
Narzędzia do ataku

- **Monitoring sieci** – airodump-ng, autorski sniffer, kismet, airgeddon;
- Ataki **Denial of Service** – mdk4, airgeddon;
- **Łamanie haseł** – wifite, airgeddon, autorski handshake capture, fluxion;
- **Złośliwy AP** – berate_ap, wifiphisher, airgeddon, fluxion;
- **Ataki na użytkowników** – wireshark, bettercap.

Narzędzie z pakietu **'Aircrack-ng'** do monitorowania i przechwytywania ruchu w sieciach Wi-Fi.

Autorskie skrypty do wykrywania adresów MAC urządzeń oraz sieci Wi-Fi w okolicy.

Kismet - profesjonalne narzędzie do monitorowania sieci Wi-Fi i urządzeń Bluetooth z funkcją mapowania.



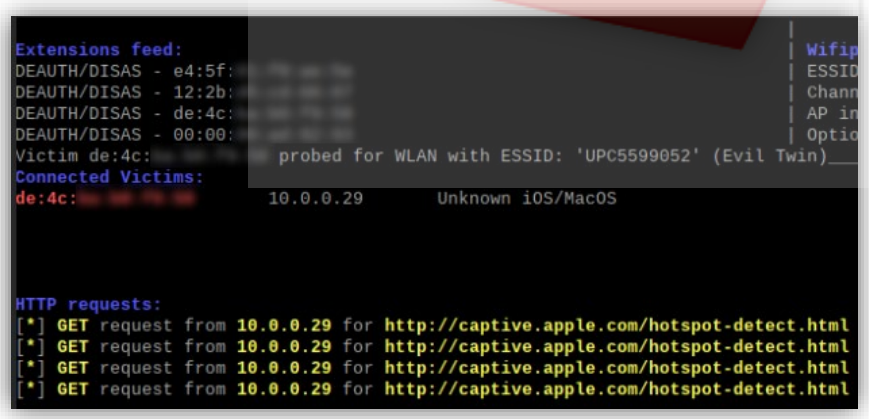
Aplikacja wykrywająca sieci radiowe wraz z mapą

Berate_ap - tworzenie fałszywych punktów dostępowych do przechwycenia ruchu użytkowników.

Wifiphisher - ataki typu 'man-in-the-middle', techniki socjotechniczne i phisingowe wykorzystujące fałszywe punkty dostępowe.

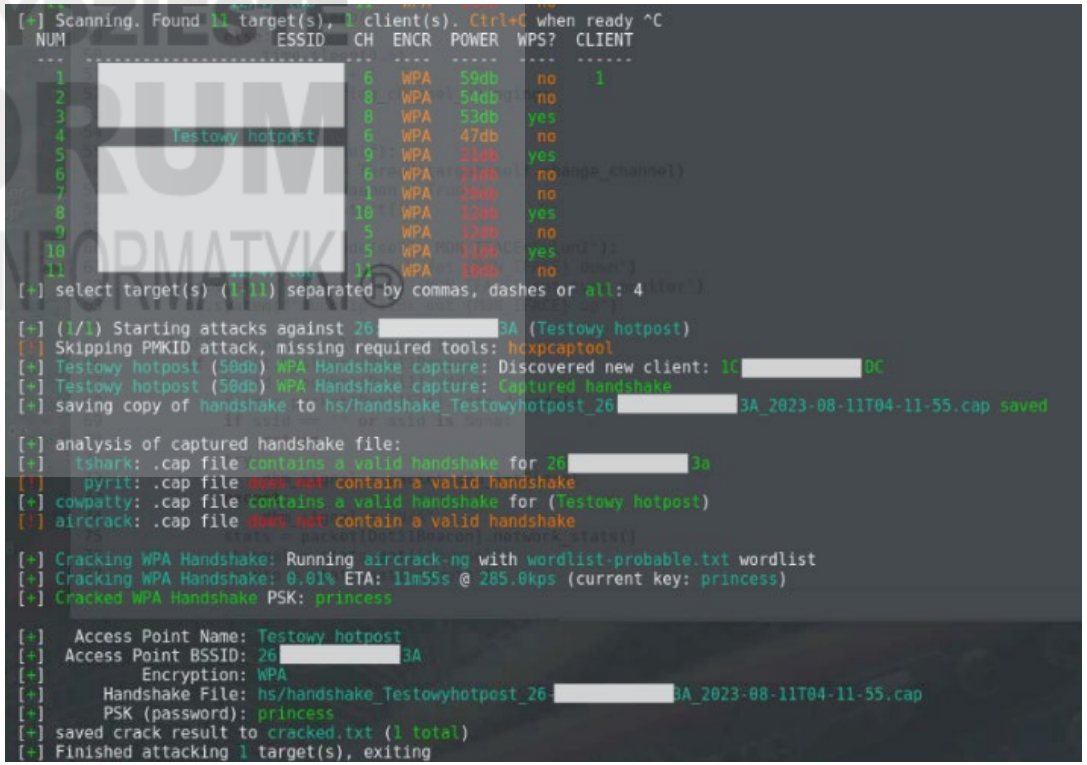
Airgeddon - tworzenie złośliwego AP z captive portalem - strony skłaniającej do podania danych.

Fluxion - ataki 'man-in-the-middle' wykorzystujące fałszywe punkty dostępowe, podobne w funkcjonalności do wifiphisher'a.

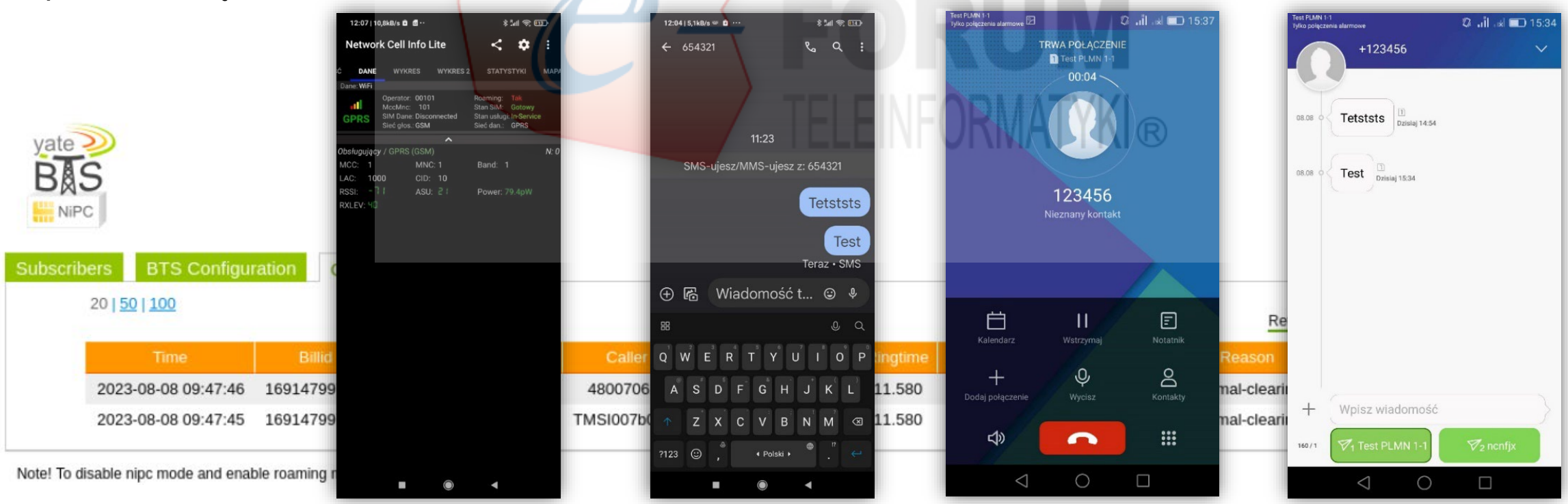


Autorskie rozwiązanie - zaawansowane narzędzie umożliwiające przechwytywanie transmisji i złamanie dostępu do sieci Wi-Fi poprzez deautentykację użytkowników i przechwycenie handshake-ów.

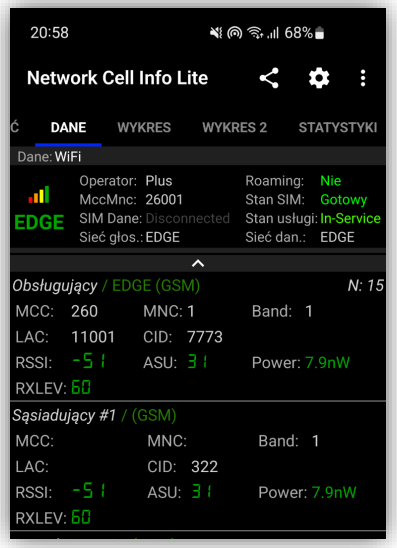
Wifite - automatyczne narzędzie do łamania zabezpieczeń sieci Wi-Fi, które wykorzystuje różne techniki ataków na hasła dostępowe.

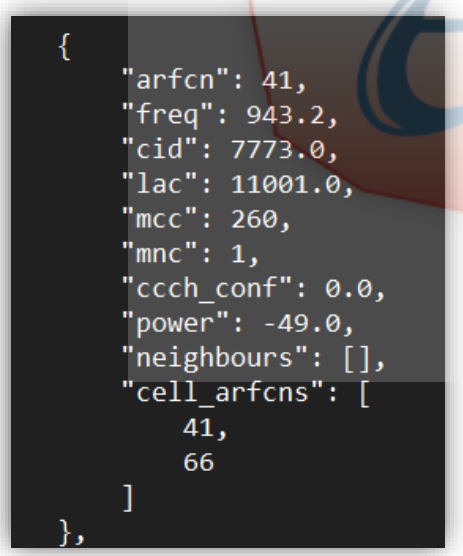


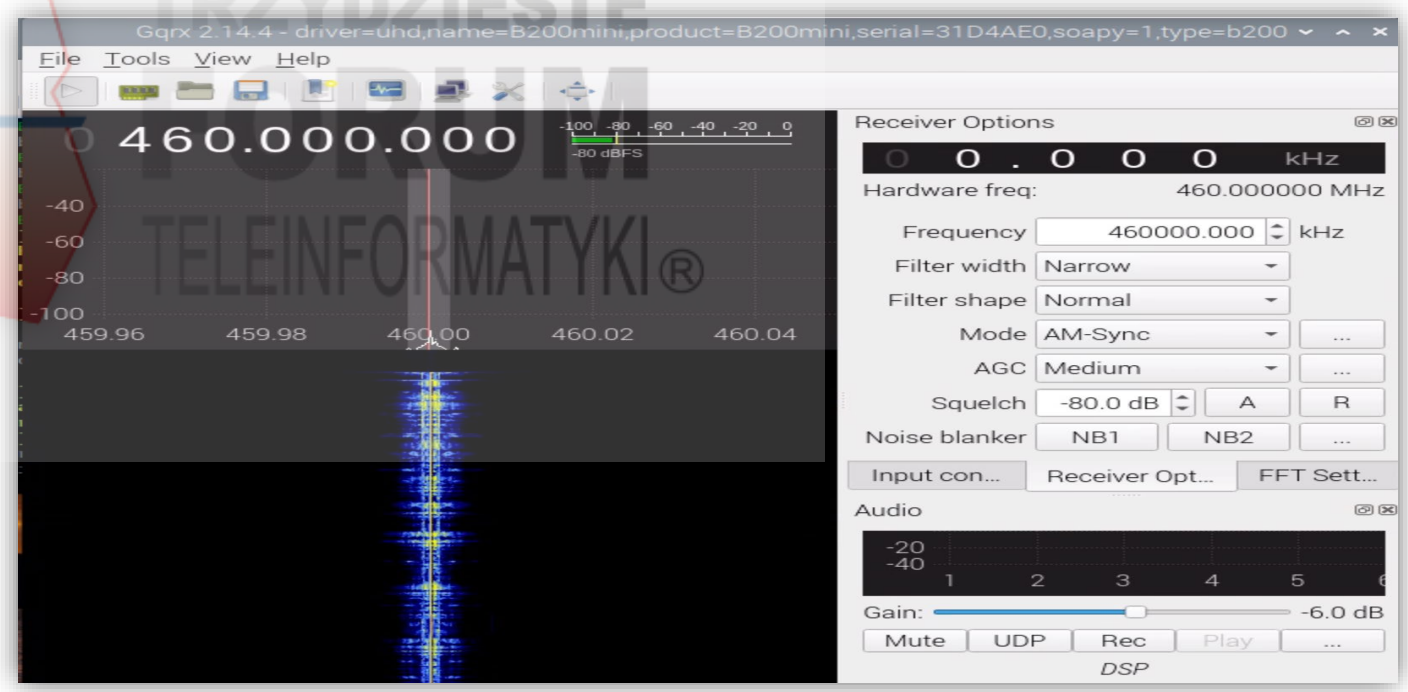
YateBTS to otwarta i elastyczna platforma oprogramowania, która umożliwia tworzenie stacji bazowych telefonii komórkowej opartych na standardach GSM, 2G, 3G, 4G LTE oraz 5G. Działa jako oprogramowanie do **wirtualizacji stacji bazowych**, pozwalając na emulację funkcji tradycyjnych stacji bazowych kompatybilnych z różnymi generacjami sieci mobilnych. YateBTS jest często wykorzystywane w celu tworzenia **prywatnych sieci komórkowych**, testowania i badania sieci mobilnych, a także w projektach związanych z komunikacją bezprzewodową.



IMSI catcher to aplikacja służąca do przechwytywania numeru IMSI (International Mobile Subscriber Identity) urządzeń komórkowych, takich jak telefony komórkowe lub modemy. Numer IMSI to unikalny identyfikator przypisany do każdej karty SIM lub urządzenia komórkowego. IMSI-catcher działa poprzez symulowanie działania nadajnika komórkowego i przyciąganie urządzeń w zasięgu, co umożliwia **zbieranie informacji o numerach IMSI** i innym ruchu komórkowym.



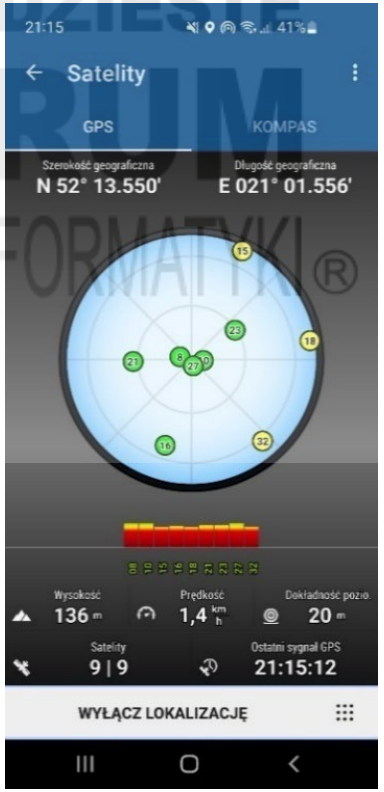


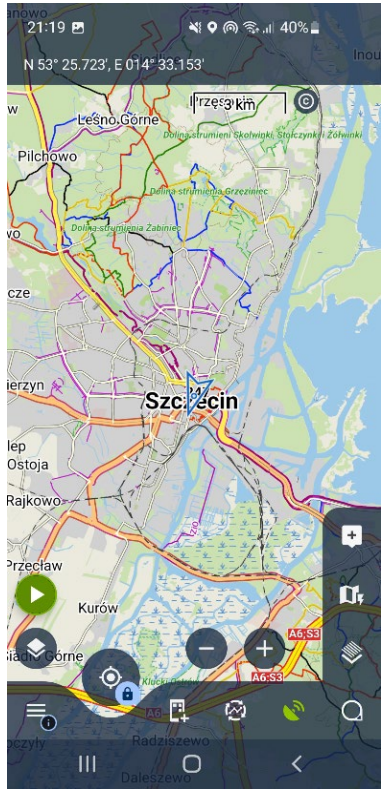


Spoofing GPS

System GPS jest powszechnym i znanym systemem satelitarnym wykorzystywanym przede wszystkim do określania pozycji oraz ustalania wzorcowego czasu dla różnych systemów technicznych.

Możliwość wygenerowania i wyemitowania dowolnego sygnału GPS wskazującego na wybraną lokalizację oraz czas pozwala na wprowadzenie **zakłócenia dla systemów lokalizacyjnych** oraz wszelkich technicznych korzystających z GPS jako podstawy czasowej.





Zastosowanie w obszarze obronności i bezpieczeństwa RP

Zaproponowany Bezzałogowy System do Rozpoznania i Ataku Sieci Radiowych **HackBee** pozwala na wykrycie oraz rozpoznanie potencjalnych zagrożeń telekomunikacyjnych, a także na przeprowadzanie ataków na sieci radiowe. HackBee może być wykorzystywany w wielu obszarach związanych z obronnością i bezpieczeństwem RP, m. in.:

- **Cyberbezpieczeństwo;**
- **Rozpoznanie radiowe;**
- **Kontr-rozpoznanie radiowe;**
- **Operacje specjalne;**
- **Wsparcie działań bojowych;**
- **Bezpieczeństwo kryzysowe;**
- **Monitoring bezpieczeństwa na granicy.**

Przedstawiony BSP **HackBee** do **rozpoznania** i **ataku sieci radiowych** jest ważnym narzędziem pozwalającym na realizację zadań z zakresu obronności i bezpieczeństwa państwa.

Rozwój systemu wychodzi naprzeciw szybko rozwijającej się **walce cybernetycznej** oraz coraz częściej wykorzystywanym technologiom wykorzystujących **bezpilotowe statki powietrzne**.

TRZYDZIESTE FORUM TELEINFORMATYKI®

Dziękujemy za uwagę

HACKBEE