Tutorial

Monitoring stacji bazowych telefonii komórkowej

Opracował: Krzysztof Niemczyk

[k.niemczyk@btsearch.pl]

2009-06-13

Wersja: 1.05

Spis treści

I. Wstęp do monitoringu – podstawowe informacje dot. stacji bazowych

BUDOWA STACJI BAZOWEJ:

Stacja przekaźnikowa (**BTS** ang. Base Transceiver Station, stacja bazowa) – w systemach łączności bezprzewodowej GSM jest urządzeniem wyposażonym m.in. w anteny fal elektromagnetycznych, łączącą telefon komórkowy, zwany w terminologii fachowej terminalem ruchomym, z częścią stałą cyfrowej sieci telekomunikacyjnej. Na dalszych odcinkach tej sieci (do centrali BSC - Base Station Controller w GSM i RNC – Radio Network Controller w UMTS) sygnał transmitowany jest za pośrednictwem światłowodu lub radiolinii. W systemie WCDMA (UMTS/3G) odpowiednikiem **BTS** jest **NodeB**, który jest traktowany jest jako medium komunikacji pomiędzy terminalem a siecią i pełni mniej funkcji w stosunku do swojego odpowiednika w GSM.

Anteny umieszczane są najczęściej w najwyższych punktach danego obiektu – tj. stalowego masztu, betonowego / metalowego słupa czy komina. Mogą być także umieszczane na dachach i elewacjach budynków, wieżach kościołów, a także wewnątrz budynków – pracując jako tzw. pikokomórki lub też na zewnątrz budynku zawieszone na niskiej wysokości pracując z obniżoną mocą jako tzw. mikrokomórki. Przy pomocy odpowiednich kabli tzw. feederów są łączone ze sprzętem znajdującym się u podnóża obiektu.

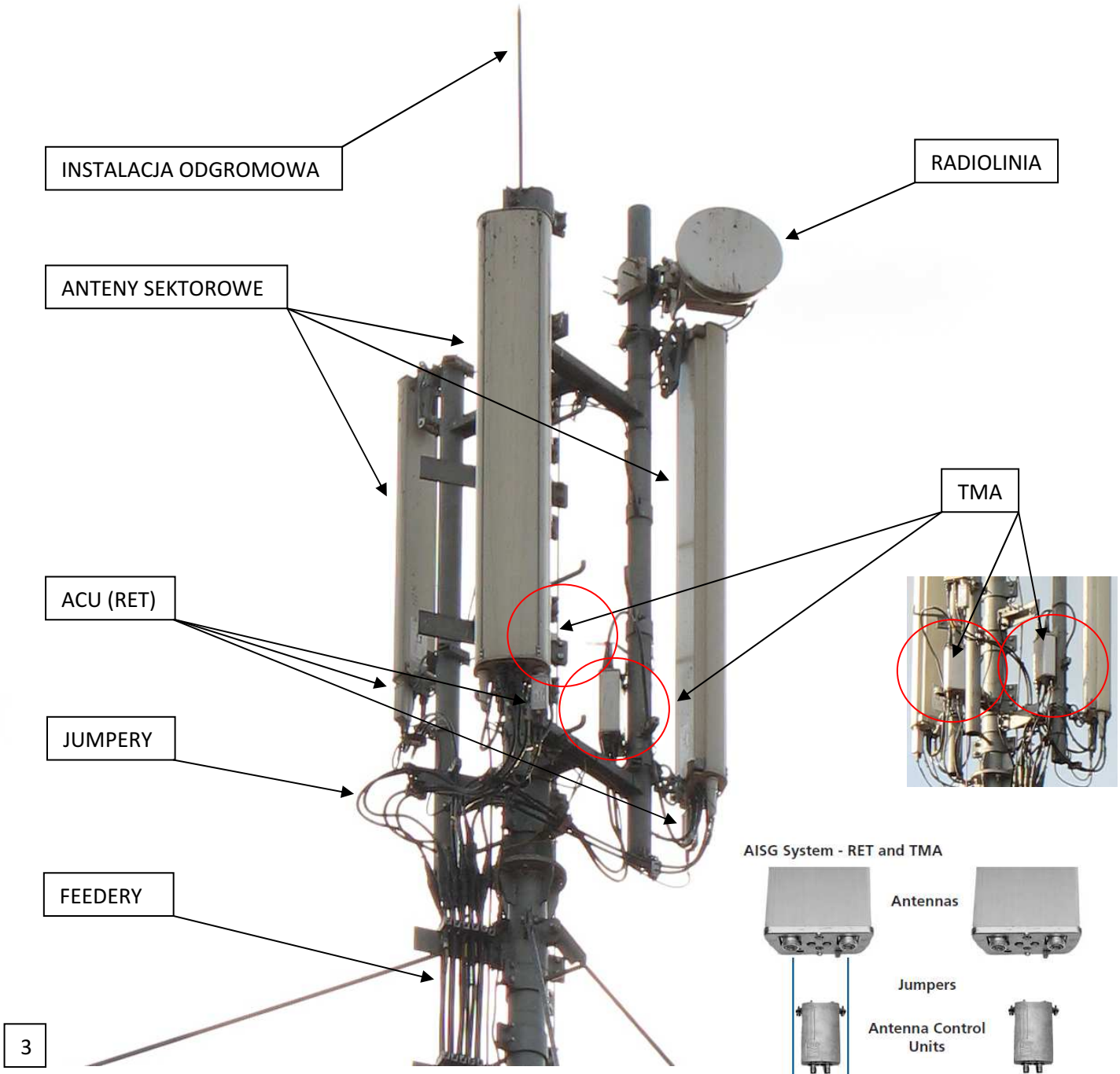
Przykłady obiektów, na których znajdują się m.in. stacje bazowe telefonii komórkowej:

Zdjęcie nr 1 – Kłodne – g. Kłodne – maszt PTK Centertel, zdjęcie nr 2 – Kraków - ul. Gaik 7 – kościół (wieża)

1

2

Zdjęcie nr 3: stacja bazowa sieci Plus – Kraków - ul. Żabiniec 45 - budynek mieszkalny:



Feedery, czyli niskostratne kable współosiowe, łączą anteny znajdujące się przeważnie na szczycie obiektu z urządzeniami stacji bazowej, które najczęściej są schowane wewnątrz specjalnej szafy lub kontenera znajdującego się u podnóża tego obiektu. Tuż przed antenami feedery rozdzielają się w dwa **jumpery** przesyłające sygnał o innej polaryzacji. Kable te mają większą elastyczność umożliwiając bezproblemowe podłączenie do kolejnych elementów. Jumpery podłączone są albo bezpośrednio do anten lub wcześniej do elementu **TMA – Tower Mounted Amplifier**, służącego do niskoszumowego wzmocnienia sygnału przy użyciu odpowiednich filtrów, w celu zrekompensowania strat przy przesyłaniu sygnału w feederach i rozgałęźnikach. W Polsce element ten stosowany jest głównie przez stacje

bazowe na których działa dodatkowo sygnał UMTS/3G. Dla stacji pracujących w paśmie GSM stosuje się elementy **MHA – Mast Head Amplifiers**, raczej rzadko stosowane w Polsce.

Do anten mogą być także podłączone także inne elementy zwane **Antenna Control Units** (inaczej nazywany też **Radio Control Units**), takie jak na przykład: **RET (Remote control of the Electrical down Tilt)** służący do zdalnej, elektrycznej regulacji pochylenia wiązki sygnału emitowanego przez anteny czyli tzw. elektryczny tilt.

Stacja bazowa z poprzedniego przykładu pracuje w konfiguracji: dwie anteny GSM 900 + UMTS, jedna antena GSM 1800 + UMTS. Do anten (GSM 900 + UMTS) są przyłączone 2 elementy TMA. Z dolnego kontenera na sprzęt prowadzonych jest 5 feederów dla każdego z pasma i sektora z osobna oraz cienki kabel na radiolinię. Dla anteny pracującej w pasmach GSM 1800 i UMTS przeznaczony jest jeden fedder, po rozdzieleniu w jumpery wpinany jest do anteny bez użycia TMA. W przypadku pozostałych fedderów w górnej części stacji bazowej następuje rozdzielenie na jumpery, które częściowo są albo wpięte bezpośrednio w anteny albo jeszcze przez element TMA (2 pary jumperów). Do każdej z anten wpinane są więc 4 lub 2 jumpery. Z obu elementów TMA wychodzą także kable do obsługi RETów anten GSM 900 + UMTS. Z jednego z elementów RET dla anten z pasm GSM 900 + UMTS wychodzi dodatkowy kabel do obsługi RETa anteny GSM 1800 + UMTS.

W Polsce najczęściej stosowane są anteny firm Kathrein i Powerwave, zaś anteny radioliniowe takich producentów jak Andrew czy Nera. Na stronach producentów anten w specyfikacjach znajdziemy dokładne informacje o portach wejściowych anten używanych dla konkretnego pasma, o zakresie częstotliwości pracy czy charakterystyce promieniowania. W przypadku anten pracujących w pasmach i GSM 900 i GSM 1800, sygnał prowadzony jest po tych samych feederach.

NAJCZĘŚCIEJ WYKORZYSTYWANE KONFIGURACJE STACJI BAZOWYCH:

	Najczęściej wykorzystywane anteny:	**Opis:**
1	Anteny kierunkowe (panelowe)	Pokrycie przez antenę określonego kierunku, ograniczonego kątem promieniowania anteny. W ramach stacji bazowych stosuje się konfiguracje 1,2,3, a nawet 4 anten pracujących w danym paśmie, skierowanych w różnych kierunkach, czyli o różnych azymutach. Jest to najczęściej stosowany rodzaj anteny w stacjach bazowych
2	Anteny dookólne	Emitowana przez antenę wiązka promieniowania przez antenę jest identyczna w każdym kierunku promieniowania. Antena ta przyjmuje zwykle postać prostego, metalowego pręta.
3	Anteny pracujące na małym obszarze	Pokrycie małego obszaru na zewnątrz budynku (mikrokomórki) oraz wewnątrz budynków (pikokomórki)
	Najczęściej wykorzystywane konfiguracje układu anten:	**Opis:**
1	Układ **space diversity**	Odbiór sygnału za pomocą dwóch (lub więcej) anten oddalonych od siebie o pewną odległość i skierowane w tym samym kierunku, tworzące wspólnie jeden 1 sektor
2	Układ **cross-polar**	Pojedyncza antena tworzy jeden sektor i jest odpowiedzialna za odbiór oraz nadawanie sygnału jednocześnie

Sektor to układ anten skierowanych w danym kierunku, odpowiedzialny za transmisję w danym paśmie.

Aktualnie większość operatorów buduje stacje bazowe posiadające anteny pracujące w paśmie GSM900 i GSM1800 razem, zaś antena UMTS dodawana jest osobno. Stosunkowo często spotykaną konfiguracją są anteny pracujące od razu we wszystkich pasmach jednocześnie, tj. GSM900, GSM1800 i UMTS. W Orange często spotykaną konfiguracją jest jedna antena pracująca na częstotliwościach GSM900 i UMTS, druga zaś odpowiedzialna za pasmo GSM1800.

Przegląd wybranych konfiguracji przedstawiono poniżej:


4


5


6


7


8


9

	Najczęściej wykorzystywane konfiguracje anten:	Lokalizacja:
4	3 **anteny kierunkowe** dla pasma UMTS (górna część masztu) 3 **anteny kierunkowe** dla pasma GSM (GSM 900 i GSM 1800) (poniżej)	T-Mobile – Kraków – ul. Czerwieńskiego 3 - hurtownia
5	**Antena typu „chorągiewka”** pracująca jako mikrokomórka zewnętrzna dla pasma GSM (GSM 1800)	Orange – Kraków – ul. Starowiślna 62 – salon Orange (elewacja)
6	**2 Anteny dookólne** dla pasma GSM (GSM 1800) w układzie space diversity	Orange – Kraków – ul. Glinik 66A - maszt własny
7	3 **anteny kierunkowe** pracujące w paśmie GSM i UMTS	Plus – Kraków – ul. Na Błonie 26 - budynek
8	Antena pracująca jako **pikokomórka wewnętrzna** dla pasma GSM (GSM 900) podwieszana pod sufitem danego pomieszczenia	Orange – Morskie Oko – schronisko (repeater)
9	6 **anten kierunkowych** (po dwie w każdym kierunku), każda może pracować w pasmach: GSM900+GSM1800+UMTS. Aktualna konfiguracja: węższa antena – pasma GSM 900 i UMTS, szersza antena pasmo GSM 1800	Orange – Kraków - al. Modrzewiowa 23 - szkoła

CZĘSTOTLIWOŚCI WYKORZYSTANE W TELEFONII KOMÓRKOWEJ:

W Polsce stosowane są technologie: GSM na częstotliwości 900 MHz i na 1800 MHz (dawna nazwa DCS, aczkolwiek technologicznie identyczne z GSM) oraz UMTS na 2100 MHz (telefonia trzeciej generacji – 3G). Czym wyższa częstotliwość, tym sygnał jest bardziej tłumiony, dlatego też w przypadku pasma GSM w dużych miastach stosowane są głównie stacje GSM 1800 w celach zwiększenia pojemności sieci, natomiast pasmo GSM 900 wykorzystywane jest głównie do zapewnienia pełnego pokrycia. Poza dużymi miejscowościami głównie stosowane są konfiguracje GSM 900. W przypadku sieci Orange, który ma najmniejszą liczbę kanałów GSM900, wiele stacji poza dużymi miejscowościami skonfigurowana jest do pracy dualnej (GSM 900/1800). Pasmo UMTS na częstotliwości 2100 MHz, z powodów ekonomicznych, jest w głównej mierze stosowane w większych miejscowościach, ponieważ dla zapewnienia pokrycia UMTS/3G porównywalnego z GSM, należy wybudować znacznie gęstszą sieć stacji bazowych. W przyszłości mniejsze miejscowości mają być pokryte sygnałem UMTS pracującym w paśmie 900 MHz.

W systemie **GSM na częstotliwości 900 MHz (GSM 900)** wykorzystywane są częstotliwości w paśmie 890 MHz do 915 MHz w kierunku stacji bazowej (uplink), natomiast w kierunku terminala (downlink) w paśmie 935 MHz do 960 MHz. Pasmo częstotliwości GSM 900 jest rozłożone na 125 kanałów o szerokości 200 kHz. Kanały przyznawane są wg. wzoru: $f_n = 890 + n * 0,2$ MHz, $f_n = 935 + n * 0,2$ MHz, gdzie fn to początek danego kanału.

Uzupełnieniem GSM'u jest tzw. **E-GSM**, który wykorzystuje dodatkowe pasma częstotliwości: 880 MHz – 890 MHz oraz 925 – 935 MHz, powodując zwiększenie liczby kanałów o dodatkowe 50. Kanały te liczone są od wartości: 975 do 1023 wg. wzoru: $f_n = 890 + (n - 1024) * 0,2$ MHz, $f_n = 935 + (n - 1024) * 0,2$ MHz, gdzie fn to początek danego kanału o szerokości 200 kHz (0,2 MHz). Większość telefonów produkowanych od paru lat wspiera E-GSM. Poza nowymi częstotliwościami technicznie E-GSM niczym nie różni się od GSM 900 czy 1800.

W przypadku systemu **GSM na częstotliwości 1800 MHz (GSM 1800, dawniej nazywany DCS)** wykorzystywane są częstotliwości w paśmie 1710 MHz do 1785 MHz w kierunku stacji bazowej (uplink) oraz w kierunku terminala (downlink) w paśmie 1805 MHz do 1880 MHz. Pasmo częstotliwości GSM 1800 jest rozłożone na 374 kanałów o szerokości 200 kHz, tak jak w GSM 900. Kanały przyznawane są wg. wzoru: fn = 1710 + (n - 511) * 0,2 MHz, fn = 1805 + (n - 511) * 0,2 MHz, gdzie fn to początek danego kanału.

Do działania systemu **UMTS** niezbędne są kanały o szerokości 5 MHz. Istnieją dwa rodzaje transmisji: FDD – Frequency Division Duplex – osobne częstotliwości dla downlink i uplink oraz TDD - Time Division Duplex - dupleks z podziałem czasowym, używany głównie w pikokomórkach i mikrokomórkach do transmisji niesymetrycznej. W Polsce wykorzystywany jest UMTS na częstotliwości 2100 MHz z 12 dupleksowymi kanałami z zakresu od 1920,5 MHz do 1979,7 MHz i stowarzyszonym pasmem 2110,5 – 2169,7 MHz dla transmisji FDD oraz 1900,1-1920,1 MHz dla transmisji w trybie TDD (4 kanały 5 MHz).

Liczba kanałów przyznanych operatorom telefonii komórkowej w Polsce:

Operator \ Technologia	GSM 900	GSM 1800	E-GSM	UMTS
Plus	45	48	-	3x5MHz (FDD) + 1x5MHz (TDD)
T-Mobile	45	48	-	3x5MHz (FDD) + 1x5MHz (TDD)
Orange	34	48	-	3x5MHz (FDD) + 1x5MHz (TDD)
Play	-	-	25	3x5MHz (FDD) + 1x5MHz (TDD)
Aero 2 Sp. z o.o.	-	-	25	-
CenterNET	-	49	-	-
Tolpis - Mobyland	-	49	-	-

Przyznane częstotliwości dla pasma GSM 900:

Operator	Liczba kanałów	Przedział częstotliwości (częstotliwość początku 1-go kanału i końca ostatniego kanału)	Numeracja kanałów w GSM
Plus	45	890,1 – 892,9 MHz (uplink) 935,1 – 937,9 MHz (downlink)	1-14
		897,3 – 903,5 MHz (uplink) 942,3 – 948,5 MHz (downlink)	37-67
T-Mobile	45	892,9 – 897,3 MHz (uplink) 937,9 – 942,3 MHz (downlink)	15-36
		903,5 – 908,1 MHz (uplink) 948,5 – 953,1 MHz (downlink)	68-90
Orange	34	908,1 – 914,9 MHz (uplink) 953,1 – 959,9 MHz (downlink)	91-124

Przyznane częstotliwości dla pasma E-GSM:

Operator	Liczba kanałów	Przedział częstotliwości (częstotliwość początku 1-go kanału i końca ostatniego kanału)	Numeracja kanałów w GSM
Play	25	880,1 – 885,1 MHz (uplink) 925,1 – 930,1 MHz (downlink)	975-999
Aero 2 Sp. z o.o.	25	885,1 – 889,9 MHz + 889,9 MHz – 890,1 MHz (uplink) 910,1 – 934,9 MHz + 934,9 MHz – 935,1 MHz (downlink)	1000-1023 i 0

Przyznane częstotliwości dla pasma GSM 1800:

Operator	Liczba kanałów	Przedział częstotliwości (częstotliwość początku 1-go kanału i końca ostatniego kanału)	Numeracja kanałów w GSM
Plus	48	1757,3 – 1759,9 MHz (uplink) 1852,3 – 1854,9 MHz (downlink)	749-760
		1777,5 – 1784,9 MHz (uplink) 1872,5 – 1879,9 MHz (downlink)	850-885
T-Mobile	48	1754,7 – 1757,3 MHz (uplink) 1849,7 – 1852,3 MHz (downlink)	736-747
		1769,9 – 1777,3 MHz (uplink) 1864,9 – 1872,3 MHz (downlink)	812-847
Orange	48	1760,1 – 1769,9 MHz (uplink) 1855,1 – 1864,9 MHz (downlink)	763-810
CenterNet S.A.	49	1710,1 – 1719,9 MHz (uplink) 1805,1 – 1814,9 MHz (downlink)	512-560
Mobyland Sp. z o.o. (Tolpis)	49	1720,1 – 1729,9 MHz (uplink) 1815,1 – 1824,9 MHz (downlink)	562-610

Przyznane częstotliwości dla pasma UMTS 2100 (kanały ok. 5MHz):

Operator	Liczba kanałów	Przedział częstotliwości (częstotliwość początku 1-go kanału i końca ostatniego kanału)
Plus	3xFDD (dupleksowe) i 1xTDD	FDD: 1950,1-1964,9 MHz (uplink) 2140,1-2154,9 MHz (downlink) TDD: 1905,1-1910,1 MHz
T-Mobile	3xFDD (dupleksowe) i 1xTDD	FDD: 1935,3-1950,1MHz (uplink) 2125,3-2140,1 MHz (downlink) TDD: 1910,1-1915,1 MHz
Orange	3xFDD (dupleksowe) i 1xTDD	FDD: 1920,5-1935,3 MHz (uplink) 2110,5-2125,3 MHz (downlink) TDD: 1915,1-1920,1 MHz
Play	3xFDD (dupleksowe) i 1xTDD	FDD: 1964,9-1979,7 MHz (uplink) 2154,9-2169,7MHz (downlink) TDD: 1900,1-1905,1 MHz

W przyszłości technologie GSM 900, GSM 1800, E-GSM mogą być zastąpione technologią UMTS pracując na częstotliwościach drugiej generacji (GSM). Wymagane będzie wtedy użycie całego pasma 5 MHz na potrzeby UMTS. W planach sieci Play jest wykorzystanie pasma 5 MHz dla potrzeb GSM w dużych miastach, natomiast poza nimi ma być uruchomiony UMTS na 900 MHz. Niestety nie ma możliwość współdziałania zarówno GSM jak i UMTS na tej samej częstotliwości na tym samym terenie.

W przypadku sieci UMTS poszczególne kanały mogą być wykorzystywane w różny sposób. Kolejne nośne (kanały FDD) mogą być uruchomione na przykład w celu oddzielenia transmisji danych HSDPA od pozostałych usług. W zależności od konfiguracji stosowanej przez operatora, określone nośne mogą być wykorzystywane tylko w czasie transmisji danych tj. momencie nawiązania połączenia typu data (czyli np. połączenia z siecią Internet) następuje przerzucenie na inną nośną – brak możliwości logowania i pozostania w trybie standby.

Numery częstotliwości kanałów sieci UMTS w paśmie 2100 MHz używanych przez polskich operatorów (widoczne są jedynie w netmonitorach takich jak FTD Nokii):

Operator	Nr częstotliwości nośnej (FDD)	Przeznaczenie / Uwagi
Plus	**10737**	Standardowa częstotliwość nośna
	10762	Uruchomiona na większości stacji, przygotowana dla transmisji danych HSDPA, można się do niej bezpośrednio zalogować
	10713	Uruchomiona na niektórych stacjach, brak informacji o przeznaczeniu, można się do niej bezpośrednio zalogować
T-Mobile	**10680 lub 10688**	Standardowa częstotliwość nośna
	10647 lub 10665/10663	Uruchomiona na niektórych stacjach, dla transmisji danych HSDPA, można się do niej bezpośrednio zalogować
	10639	Nośna dodatkowa
Orange	**10564**	Standardowa częstotliwość nośna
	10589	Uruchomiona na wszystkich stacjach, dla transmisji danych HSDPA, Nie zawsze można się do niej bezpośrednio zalogować – przerzucanie tylko w trakcie transmisji danych
	10614	Pod HSPA+ DC z 10589
Play	**10836**	Standardowa częstotliwość nośna
	10787	Uruchomiona na niewielu stacjach, oddalonych od siebie o sporą odległość, w celu pokrycia dużego obszaru danym sektorem, można się do niej bezpośrednio zalogować
	10812	Nośna dodatkowa, uruchomiona w celach pojemnościowych

W przypadku sieci GSM, w ramach jednego sektora przyznawane jest wiele kanałów, tzw. TRX'ów. TRX fizycznie jest modułem sprzętowym zainstalowanym wewnątrz szafki lub kontenera stacji bazowej, odpowiedzialnym za obsługę danego kanału (lub zakresu kanałów) w ramach określonego sektora stacji. Ilość TRX'ów obsługujących dany sektor jest uzależniona w głównej mierze od ruchu generowanego w pokrywanym przez ten sektor obszarze, aczkolwiek w terenach o „średnim” obciążeniu przeważnie są to 3 TRX'y na sektor. Każdy kanał dzielony jest na 8 timeslotów, w których jeden zajmuje się sygnalizacją, pozostałe wykorzystywane są do rozmów lub transmisji danych. Timesloty to szczeliny czasowe, w których dany terminal może transmitować dane. W przypadku, gdy sektorowi przyznane są 3 kanały, najczęściej tylko jeden timeslot (TS) wykorzystywany jest do celów sygnalizacyjnych, choć w dużej mierze zależy to od rodzaju ruchu na danym obszarze i ilości przyznanych kanałów. W czasie rozmowy wykorzystywany jest jeden TS, choć w przypadku problemów z pojemnością stacji bazowej, operator może wymusić pracę przy pomocy połowy timeslota. Mamy wówczas do czynienia z kodowaniem Half Rate (HR), co z jednej strony powoduje pogorszenie jakości rozmów, ale z drugiej ofertuje dwukrotnie większą pojemność danego kanału, bowiem jest on wówczas w stanie obsłużyć co najmniej 14 zamiast 7 użytkowników jednocześnie W przypadku transmisji danych

może być wykorzystane więcej kanałów i lepszą oraz inną modulację, powodując zwiększenie prędkości transmisji tj. przepustowości łącza. W sieci Plus, rzadziej w Orange przyznane kanały dla danego sektora nie pracują w tym samym paśmie częstotliwości. Zdarza się, iż kanał z timeslotem do celów sygnalizacyjnych pracuje w paśmie GSM 900, zaś w czasie rozmowy wykorzystywane są kanały także pracujące w GSM 1800, co można zobaczyć jedynie w bardziej zaawansowanych netmonitorach.

W przypadku sieci UMTS nie istnieje podział na timesloty. Transmisja polega tutaj na przypisaniu poszczególnym użytkownikom korzystającym z tego samego kanału do przesyłania danych sekwencji rozpraszających, dzięki którym odbiornik jednoznacznie zidentyfikuje przeznaczoną dla niego transmisję. Z danego kanału częstotliwości może korzystać wiele użytkowników jednocześnie. Stacje bazowe są odróżniane za pomocą numerów identyfikatorów stanowiących sumę PSC i SSC - PSC (Primary Synchronization Code) i SSC (Secondary Synchronization Code) o długości 256 czipów każdy. Jeden czip to jeden znak sygnału źródłowego przemnożonego przez sekwencję rozpraszającą). Identyfikatory te widoczne są tylko w zaawansowanych netmonitorach.

Główne parametry stacji bazowych możliwe do podglądnięcia w programach i zaawansowanych netmonitorach:

- **CellId (CID - Cell Identifier)** – identyfikator komórki (sektora) stacji bazowej do której aktualnie jesteśmy zalogowani, dla każdego sektora danego pasma przyznane jest inne CellId. W przypadku, gdy korzystamy z sieci UMTS/3G istnieje dodatkowo numer **RNC (Radio Network Controller)**, czyli kontrolera stacji bazowych UMTS – NodeB. Stosowany jest następujący wzór do wyliczenia długiego, zbiorczego CellId: DŁUGI_CELLID = RNC * 65536 + KRÓTKI_CELLID. W przypadku sieci 3G, dany sektor dla każdej częstotliwości nośnej ma przyznane inny numer CellId.

  Monitory sieci przeważnie pokazują CID w postaci „długiej", z którego można obliczyć CID krótki oraz RNC:
  KRÓTKI_CELLID = operacja modulo 65536 (mod 65536) z DŁUGI_CELLID
  RNC = liczba całkowita z wyniku operacji DŁUGI_CELLID / 65536

  Lub rozbijając „długi" CID wg następującego schematu:
  1234567890 (dec) = 499602D2 (hex)
  Stąd:
  4 ostatnie wartości czyli 02D2 (hex) – CellId komórki => 722 (dec)
  bez 4 ostatnich wartości czyli 4996 (hex) – identyfikator RNC => 18838 (dec)

- **LAC** (**Local Area Code / Location Area Code)** – numer obszaru przywołań, numer lokalny dla grupy stacji bazowych
- numer kanału na którym pracuje dany sektor stacji bazowej (CH – channel)
- w przypadku pracy w paśmie UMTS – ID (PSC i SSC) stacji bazowej

II. Informacje dot. monitoringu stacji bazowych, dostępne aplikacje

WYKAZ STACJI BAZOWYCH – WWW.BTSEARCH.PL ORAZ POMOCNE UWAGI:

Na stronie http://www.btsearch.pl prowadzony jest wykaz stacji bazowych, prowadzony przez zwykłych użytkowników telefonii komórkowej, korzystających z dodatkowych aplikacji i przysyłających następujące informacje o stacjach bazowych:

- **Sieć**: 260 01 – Plus, 260 02 – T-Mobile, 260 03 – Orange, 260 06 – Play
- **Lokalizacja**: województwo, miejscowość, ulica, rodzaj obiektu
- **LAC** – Local Area Code / Location Area Code
- **CID** – CellId – CellIdentifier
- **pasmo** pracy stacji: GSM 900, GSM 1800, UMTS
- **RNC** dla stacji UMTS (3G)
- ewentualnie numer kanału stacji dla 3G (numer częstotliwości nośnej)

Numery dokładnych kanałów nie są dokładnie spisywane, głównie dlatego, iż konfiguracje stacji bazowych bardzo często są zmieniane. Dodatkowo darmowe, proste aplikacje nie posiadają możliwości dokładnego odczytania bardziej skomplikowanych parametrów stacji bazowej.

W przypadku sieci T-Mobile, Orange, Play – CellId powinno być unikatowe w skali kraju, w przypadku Plusa CellId jest unikatowe w obrębie każdego z czterech obszarów (pierwsza cyfra w polu LAC oznacza numer danej strefy).

CellId jest przyznawany często nietypowo dla każdego sektora stacji bazowej, czyli niezgodnie stosowaną kiedyś regułą: xxxx1-3, xxxx4-6 lub xxxx7-9. Końcówki CellId przyznawane były zgodnie ze wskazówkami zegara licząc od kąta zerowego. Głównie z powodu dużej liczby stacji w celu utrzymania przez Operatora unikalności CellId na terenie całego kraju przyznawane CellId jest dosyć chaotycznie.

Programy tupu Celltrack i PyNetMony nie pozwalają niestety na sprawdzenie, z której częstotliwości nośnej przy pracy w sieci UMTS telefon aktualnie korzysta. W przypadku Orange najczęściej druga nośna nie pozwala na zalogowanie się (przygotowana tylko na poczet transmisji HSDPA). W tym przypadku na cele bazy btserach.pl spisywane są CellId tylko dla jednej nośnej. W przypadku Plusa druga nośna ma najczęściej CellId z końcówkami 4,5,6 i początkiem takim samym jak dla defaultowej (głównej) nośnej UMTS. W przypadku Ery niestety nie każda stacja ma uruchomioną drugą nośną.

Bardzo pomocna przy monitoringu stacji bazowych może być baza stacji bazowych wydawana przez UKE - Urząd Komunikacji Elektronicznej - http://www.uke.gov.pl/uke/index.jsp?place=Lead24&news_cat_id=358&news_id=3749&layout=9&page=text. Co miesiąc pojawia się jej aktualizacja i zawiera spis stacji bazowych, które mają pozwolenie radiowe wraz z dokładnymi informacjami o: lokalizacji, współrzędnych GPS oraz StationID, czyli wewnętrzny numer stacji stosowany przez operatora. Niestety spis nie posiada takich informacji jak LAC, CellId czy RNC. Spis wydawany przez UKE jest często niestety niepełny. Brakuje w nim części działających stacji bazowych, zaś w przypadku najczęściej Plusa istnieje wiele stacji bazowych przygotowanych jedynie na papierze. Spis UKE zawiera także często błędy lokalizacji danej stacji czy

współrzędnych GPS. Na podstawie spisu UKE została przygotowana mapka stacji bazowych, która dostępna jest na stronie http://mapa.btsearch.pl. Może ona w znacznym stopniu przydać się przy monitoringu stacji bazowych.

Zgłoszenia dot. stacji bazowych na potrzeby bazy www.btsearch.pl można przesyłać na adres: btsearch@btsearch.pl

PORÓWNANIE APLIKACJI DO MONITORINGU:

Do monitoringu stacji bazowych telefonii komórkowej proponuje się wykorzystanie telefonów z systemem operacyjnym Symbian i wgranymi aplikacjami:

1. **Celltrack**
2. **PyNetMony**
3. **FTD – FieldTest (tutorial w trakcie przygotowywania)**

Monitoring stacji bazowych powinien wyglądać następująco:

- obejście danej stacji bazowej dookoła dla każdego pasma osobno i przeglądnięciu zmieniających się parametrów CellId / LAC za pomocą głównego okna lub późniejsze przeglądniecie logów. Dokładny monitoring powinien także obejmować sprawdzenie poziomu sygnału w miejscu testów, jednak z powodu ubogości aplikacji (brak możliwość dokładnego sprawdzenia poziomu sygnału), nie jest w pełni możliwy
- włączenie programów typu Celltrack lub PyNetMony przed dłuższą podróżą – np. pociągiem lub samochodem i pozostawienie aplikacji włączonej w trybie pracy w tle (uwaga na czerwoną słuchawkę dla aplikacji Celltrack pod Symbian OS 9.x – program się wyłącza). Można także wtedy włączyć urządzenie GPS, dzięki czemu będziemy wiedzieć, gdzie w przybliżeniu znajduje się nowa stacja

Najbardziej polecaną aplikacją do monitoringu typu Freeware jest Celltrack. Program PyNetMony posiada wiele narzędzi bardziej rozbudowanych, jednak część z opcji musi być niestety jeszcze poprawiona. Ogólne porównanie programów zostało przedstawione w tabeli poniżej:

APLIKACJE:	PLUSY	MINUSY
Celltrack	• łatwa instalacja • łatwość monitoringu • aplikacja typu Freeware • działa na wszystkich telefonach z konkretnym OS	• w czasie trwania rozmowy czy transmisji danych aplikacja może nie odświeżać danych • program podaje nieprawdziwe informacje o poziomie sygnał (wina Nokia API) • dla OS 9.x program po wciśnięciu czerwonej słuchawki nie przechodzi do pracy w tle, tylko się wyłącza • aktualnie rzadko aktualizowany • nie działa kanał CB z nazwą okolicy nadanej przez operatora dla Symbian OS 9.x • brak możliwości: sprawdzenia takich parametrów jak: pasmo (GSM 900 czy GSM 1800), kanału, częstotliwości nośnej dla UMTS/3G • brak możliwości „zakleszczenia” się na danym kanale lub częstotliwości nośnej (jak w programie FieldTest - funkcja BTS TEST)

PyNetMony	• bardziej rozbudowane funkcje w stosunku do Celltracka • często aktualizowany • aplikacja Freeware • bardzo dobrze sprawuje się przy pracy w tle	• w czasie trwania rozmowy / transmisji danych aplikacja może nie odświeżać danych • program podaje nieprawdziwe informacje o poziomie sygnał (wina Nokia API) • utrudniona instalacja – wiele programów, dodatkowo wymagających podpisywania • działa tylko dla Symbian OS 9.x • nie działa kanał CB z nazwą okolicy nadawanej przez operatora • brak możliwości: sprawdzenia takich parametrów jak: pasmo (GSM 900 czy GSM 1800), kanału, częstotliwości nośnej dla UMTS • brak możliwości „zakleszczenia" się na danym kanale lub częstotliwości nośnej (jak w programie FieldTest - funkcja BTS TEST) • w logach brak informacji o nazwie stacji • brak informacji o zmienionym LAC: w zależności od konfiguracji programu albo traktuje parę LAC i CellId jak nową stację albo podaje często nieprawdziwą informację o stacji z pasującym CellId (problem unikalności CellId w obrębie Polski)
FTD - FieldTest	• pełny monitoring w czasie rzeczywistym	• aplikacja płatna, praktycznie niedostępna oficjalnie (w Internecie wersje nielegalne) • brak możliwości generowania logów • nie działa na wszystkich telefonach na Symbian OS • dla Symbian OS 7.0/8.0 nie działa w trakcie transmisji danych GPRS/EDGE/UMTS

III. Instalacja programów

Celltrack:

Najnowsze wersje programu dostępne są na stronie producenta: http://www.afischer-online.de/sos/celltrack/
Program dostępny dla telefonów z systemem operacyjnym Symbian:

- OS version 6.2 - http://www.afischer-online.de/sos/celltrack/CellTrack62.SIS
- OS version 7.0/8.0 - http://www.afischer-online.de/sos/celltrack/CellTrack70.SIS
- OS version 9.x (3rd Generation) - http://www.afischer-online.de/sos/celltrack/CellTrack91_S60_3_0_v_1_0_7_unsigned.sis

Aby sprawdzić wersję OS naszego telefonu, należy np. wejść na http://www.s60.com/life/s60phones/browseDevices.do, wybrać dany model i wejść do Technical Specificaton.

W przypadku programu Celltrack dla OS version 9.x, tak jak dla innych programów, wymagany jest przed instalacją podpis programu certyfikatem. Za pomocą kombinacji *#06# odczytujemy numer IMEI naszego telefonu. Wchodzimy na https://www.symbiansigned.com/app/page/public/openSignedOnline.do, gdzie podajemy numer IMEI, adres e-

mail i aplikację, którą mamy podpisać (czyli nasz pobrany wcześniej Celltrack dla OS 9.x). Dodatkowo najlepiej zaznaczamy „Select all" w „Capability information", podajemy kod z obrazka i akceptujemy regulamin. Po chwili na podany adres e-mail powinniśmy otrzymać wiadomość z prośbą o weryfikację, a w następnej link z do podpisanej aplikacji. Instalacja programu odbywa się standardowo, tak jak w przypadku każdego programu, czyli wysyłając plik bezpośrednio przy użyciu Bluetooth lub za pomocą programu zainstalowanego na komputerze – np. Nokia PC Suite za pomocą kabla lub Bluetooth. Aplikacje instalujemy najlepiej w Pamięci telefonu, nie na karcie MMC. W przypadku problemów z instalacją programu pomimo podpisania aplikacji dla Symbian OS 9.x należy sprawdzić w ustawieniach telefonu: Ustawieniach -> Aplikacje -> Menadżer aplikacji -> Inst. Oprogramowania czy jest zaznaczona opcja **Wszystko**.

PyNetMony:

Aplikacja działa niestety tylko pod Symbian OS 9.x. Aby sprawdzić wersję OS naszego telefonu, należy np. wejść na http://www.s60.com/life/s60phones/browseDevices.do, wybrać dany model i wejść do Technical Specificaton. Najnowsze wersje programu dostępne są na stronie producenta: http://pynetmony.googlepages.com/download_py

Przed instalacją programu wchodzimy na stronę http://sourceforge.net/project/showfiles.php?group_id=154155, wybieramy Download, a później najnowszą wersję PythonForS60 z końcówką 3rdEd (aktualnie najnowsza wersja to PythonForS60_1_4_5_3rdEd.sis). Sam Python nie wymaga podpisywania certyfikatem – instalujemy od razu w telefonie Symbian OS 9.x.

Resztę niezbędnych plików znajdziemy na stronie producenta (link na początku tej części tutoriala). Pliki wymagają niestety podpisywania certyfikatem, tak jak w przypadku Celltrack (patrz na poprzednią część - Celltrack). Niestety do podpisania jest 8 plików (poza PythonForS60). Najlepiej jest w wykorzystać parę kont mailowych – istnieją ograniczenia dot. podpisywania. Można niestety podpisać 1 aplikację co ok. 3-5 minut w obrębie podanego adresu mailowego. Po podpisaniu instalujemy w telefonie wg. kolejności, na dysku C (w pamięci telefonu):

- **1.: PythonForS60_1_4_5_3rdEd.SIS (Doesn't require signing)**
- **2.: locationrequestor_3rd_unsigned.sis (http://usa.dpeddi.com/locationrequestor_3rd_unsigned.sis)**
- **3.: wlantools-PyS60_1_4_4_3rdEdFP1-OMAP2420-unsigned.sis (choose the correct version for your Mobile) (http://chris.berger.cx/uploads/PyS60/wlantools/)**
- **4.: lightblue-0.3.3-s60-3rdEd_freedevcert.sis (http://lightblue.sourceforge.net)**
- **5.: blues_3rd_1_0_0_unsigned.SIS (http://sourceforge.net/project/showfiles.php?group_id=132176)**
- **6.: envy_3rd_1_0_4_unsigned.SIS (http://sourceforge.net/project/showfiles.php?group_id=132176)**
- **7.: elocation-PyS60_1_4_5_3rdEdFP1-unsigned.sis (choose the correct version for your Mobile) (http://chris.berger.cx/uploads/PyS60/elocation/)**
- **8.:miso-1.95-s60_31_dev.sis (http://www.hiit.fi/files/fi/da/miso/utils/web/)**
- **9.: PyNetMony_2_02_03_unsigned.sis (http://pynetmony.googlepages.com)**

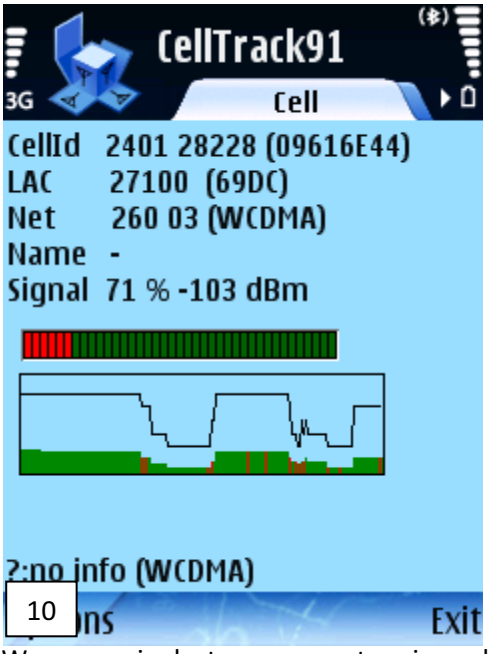
Źródło: http://pynetmony.googlepages.com/download_py

W przypadku problemów z instalacją programu pomimo podpisania aplikacji dla Symbian OS 9.x należy sprawdzić w ustawieniach telefonu: Ustawieniach -> Aplikacje -> Menadżer aplikacji -> Inst. Oprogramowania czy jest zaznaczona opcja **Wszystko**. Aplikacja instalujemy w pamięci telefonu. Dodatkowo tworzone są automatycznie foldery na karcie pamięci, do których będzie można wrzucić bazę stacji bazowych (pliki clf) czy wygenerować logi. Możliwe jest to oczywiście także na dysku C (pamięci telefonu). Szczegóły dotyczące odpowiednich ustawień w dalszej części tutoriala.

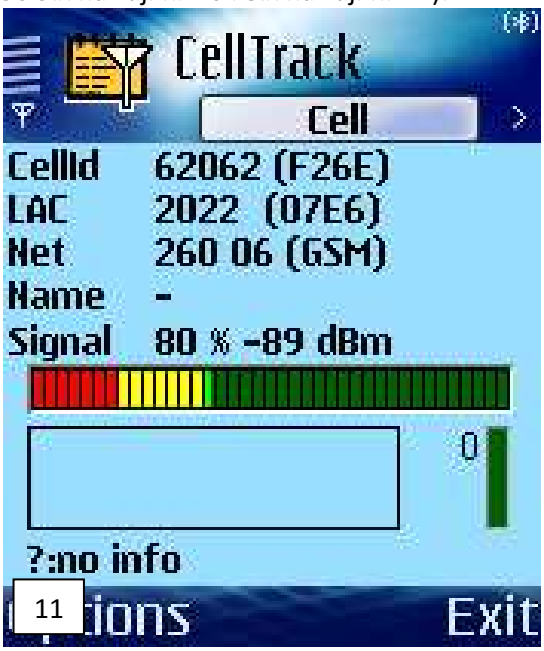
IV. Pierwsze uruchomienie programów

Celltrack:

Po uruchomieniu programu powinniśmy otrzymać (screen programu dla OS 9.x na zdj. nr 10 i 8.x na zdj. nr 11):



10



11

W programie dostępne są następujące okna:

1. okno główne – **Cell**:
   Opis wyświetlanych informacji:
   - **CellId (CID - Cell Identifier)** – numer komórki stacji bazowej do której aktualnie jesteśmy zalogowani. W przypadku, gdy korzystamy z sieci UMTS/3G w polu **Net** mamy wpisane WCDMA, a przed **CellId** znajduje się numer **RNC (Radio Network Controller)**, czyli kontrolera stacji bazowych UMTS – NodeB
   - **LAC** (**Local Area Code / Location Area Code)** – numer obszaru przywołań, numer lokalny dla grupy stacji bazowych
   - **Net** – międzynarodowy kod sieci (260 01 – Plus, 260 02 – T-Mobile, 260 03 – Orange, 260 06 – Play). Obok znajduje się informacja dot. pasma z którego aktualnie korzystamy – GSM (GSM900 lub GSM 1800) lub WCDMA (czyli UMTS/3G)
   - **Name –** informacja o sieci – pobieranie informacji dot. lokalizacji z kanału nr 50 – nie działa na OS 9.x
   - **Signal** – aktualny poziom sygnału odbieranego ze stacji do której jesteśmy zalogowani. Poziom sygnału często może pokazywać błędne informacje lub nie odświeżać się z powodu ograniczeń Nokia API
   - **wykres** – zmieniający się poziom sygnału w czasie
   - **„?:no info"** – możliwość odczytania informacji o komórce o danym numerze CellId na podstawie bazy stacji w formacie clf wgranej do programu (szczegóły w dalszej części tutoriala)
2. okno **Cell More** (po przejściu strzałką w prawo):
   Okno zawiera dokładniejsze informacje w porównaniu z głównym oknem, ale bez wykresów poziomu sygnału. W wersjach nie dla OS 9.x, widoczny jest po zalogowaniu tzw. długi CellId, który jest powiązany z RNC na podstawie zależności: DŁUGI_CELLID = RNC * 65536 + KRÓTKI_CELLID. W przypadku programu w wersji dla OS 9.x widzimy standardowo CellId jako dwie, osobne wartości (RNC i KRÓTKI_CELLID).

3. okno **CellLoc** (tylko dla Symbian OS 9.x):
   Okno to związane jest z wykorzystaniem urządzenia GPS do monitoringu. Szczegóły w następnej części.
4. okno **CellPic**:
   Do programu możliwe jest dogrywanie zdjęć stacji bazowych, nazywając zdjęcia przykładowo 256301FE26202.jpg, jeśli CellId to 2563 (przeliczone do hex), LAC 01FE (przeliczone do hex), w sieci 262 02 (czyli Cell (hex.) + LAC (hex.) + country + net). Zdjęcia wrzucamy do katalogu ze zdjęciami w folderze programu. Okno to trak taktowane jest jedynie jako „bajer".
5. okno **Phone**:
   Okno to pozwala sprawdzenie podstawowych informacji dotyczących naszego telefonu, niezwiązanych z monitoringiem stacji bazowych

PyNetMony:

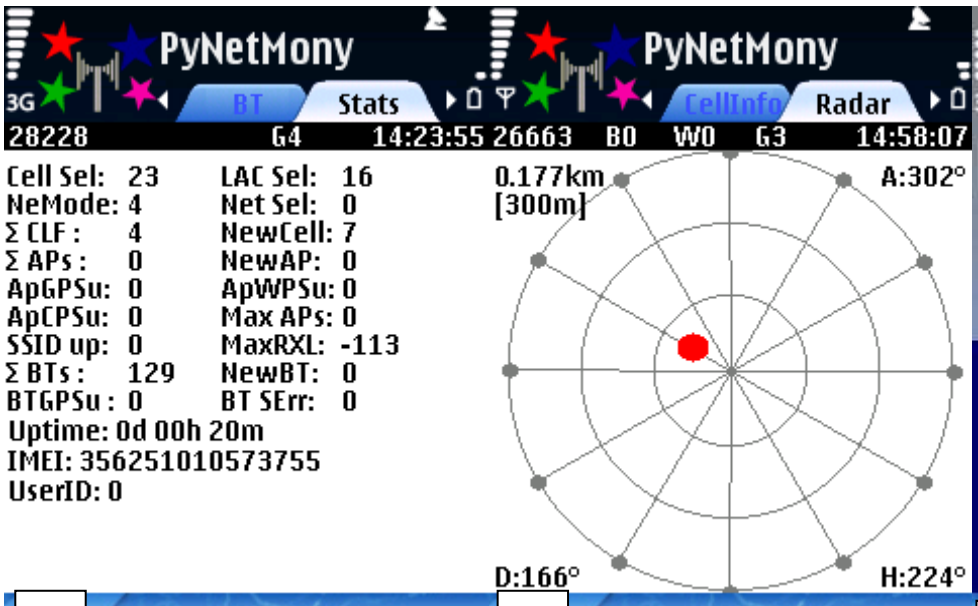
Po uruchomieniu programu powinniśmy otrzymać następujące okno (screen programu na zdjęciu nr 12):

1. okno główne – **NetMon**:
   Opis wyświetlanych informacji:
   - **CellId (CID - Cell Identifier)** – numer komórki stacji bazowej do której aktualnie jesteśmy zalogowani.
   - **godzina** – aktualny czas
   - **LCID** - DŁUGI_CELLID = RNC * 65536 + KRÓTKI_CELLID w przypadku pracy w sieci UMTS, lub krótki CID - **CellId (CID - Cell Identifier)** – numer komórki stacji bazowej do której aktualnie jesteśmy zalogowani. W nawiasie wartość przeliczona do hex.
   - **LAC** (**Local Area Code / Location Area Code)** – numer obszaru przywołań, numer lokalny dla grupy stacji bazowych
   - W przypadku, gdy korzystamy z sieci UMTS/3G pojawia się dodatkowe pole o nazwie **RNC (Radio Network Controller)**, czyli numer kontrolera stacji bazowych UMTS – NodeB
   - **Net** – międzynarodowy kod sieci (260 01 – Plus, 260 02 – T-Mobile, 260 03 – Orange, 260 06 – Play). Obok znajduje się informacja czy znajdujemy się w sieci macierzystej czy roamingu
   - **RXL** – aktualny poziom sygnału odbieranego ze stacji do której jesteśmy zalogowani. RXL często może pokazywać błędną wartość lub nie odświeżać się z powodu ograniczeń Nokia API
   - **MOD** - pasmo z którego aktualnie korzystamy – GSM (GSM900 lub GSM 1800) lub WCDMA (czyli UMTS/3G)
   - **RAM** – ilość pamięci RAM aktualnie wykorzystywanych, niezwiązane z monitoringiem sieci
   - **„New Cell..."** – informacje o stacji bazowej, możliwość odczytania informacji o komórce o danym numerze CellId na podstawie bazy stacji w formacie clf wgranej do programu (szczegóły w dalszej części tutoriala)

2. okno **Graph** (po przejściu strzałką w prawo):
   Okno zawiera zmieniający się poziom sygnału oraz informacje o stacjach bazowych w czasie (ostatnie 3,3 min.)
3. okno **History** (zdjęcie nr 13):
   Okno zawiera historię ostatnio wykorzystywanych stacji bazowych. Wartość n/a w kolumnie RNC oznacza, iż zalogowani byliśmy do stacji bazowej pracujące w paśmie GSM
4. okno **GPS** (zdjęcie nr 14):
   Okno wykorzystywane tylko z włączonym odbiornikiem GPS. Zawiera informacje dotyczące naszego położenia oraz (w przypadku dogrania plików ze stacjami bazowych wraz z ich współrzędnymi GPS) także odległość i kierunek do stacji z której aktualnie korzystamy
5. okno **WLAN**:
   Możliwość zbierania informacji o mijanych sieciach bezprzewodowych. W przypadku monitoringu sieci komórkowych, opcja nieużywana.
6. okno **CellInfo**:
   Ogólna informacja o stacji bazowej z której korzystamy
7. okno **Radar** (zdjęcie nr 16):
   W graficzny sposób rozrysowany kierunek do stacji bazowej. Wymaga dogranego pliku ze stacjami bazowymi wraz z ich współrzędnymi GPS oraz włączonego urządzenia GPS.
8. okno **Map**:
   Możliwość podejrzenia mapy okolicy w której znajduje się nasza stacja bazowa. Wymaga dogranego pliku ze stacjami bazowymi wraz z ich współrzędnymi GPS, włączonego urządzenia GPS oraz połączenia z Internetem.
9. okno **BT**:
   Możliwość zbierania informacji o mijanych telefonach z włączonym Bluetoothem. W przypadku monitoringu sieci komórkowych, opcja nieużywana.
10. okno **Stat** (zdjęcie nr 16):
    informacje liczbowe o nowych stacji bazowych, wielkości bazy clf oraz innych parametrach.
11. okno **Neighbours** (zdjęcie nr 18):
    Wyliczone odległości do najbliższych stacji bazowych. Wymaga dogranego pliku ze stacjami bazowymi wraz z ich współrzędnymi GPS oraz włączonego urządzenia GPS. Program wyliczy odległości po wejściu do Options -> Database -> Calculate Neighbour
12. okno **Newclf**:
    Podane stacje bazowe, które nie widnieją w dogranym pliku clf traktowane jako nowe stacje

13

14



15 16 17

V. Podstawowa konfiguracja programów

Celltrack:

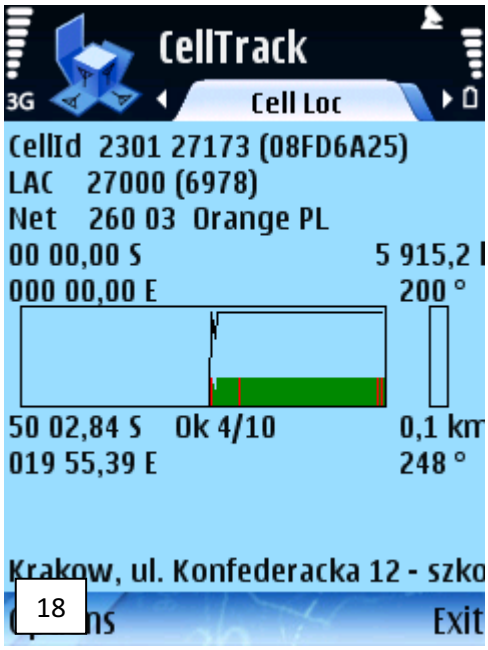
Konfigurację przeprowadzamy po wejściu **Options -> Settings** -> **Logging** lub **Display**. Konfiguracja dla menu Logging jest następująca:

- **Log Mode** – ustawiamy **Cell Changes** – wszystkie zmieniająca się sektory stacji bazowych będą spisywane do plików trace w katalogu programu. W przypadku Symbian OS 9.x powstaną pliki tracexxxxx, gdzie xxxxx to międzynarodowy numer sieci komórkowej
- **Direction supported –** opcja pozwala na pokazanie w głównym oknie z której strony widzimy stację bazową na podstawie końcówek CellId (np. stacja 3-sektorowa o CellId ma końcówki xxxx1, xxxx2, xxxx3, które przyznawane były najczęściej zgodnie ze wskazówkami zegara od kąta 0-go). Ponieważ CellId przyznawane jest aktualnie bardzo różnie, sugeruje się nie wykorzystywanie tej opcji (ustawiamy **Off**)
- **Dir. Digit Position –** ustawiamy **Off**, dla Symbian OS 9.x zostawiamy **Last Position**
- **Cell Name from Id** – ta opcja nie będzie przez nas wykorzystywana, zostawiamy **Off**
- **Cell Name from CBS** – (nie działa na Symbian OS 9.x) przed ustawieniem na **On** wyłączamy program Celltrack i wchodzimy do konfiguracji w telefonie: **Ustawienia** -> **Sieć** -> **Informacje o sieci** -> **Wyłączone**. Włączamy Celltrack i ustawiamy parametr na **On**. Od tej chwili po restarcie aplikacji na wyświetlaczu powinny być wyświetlone informacje z kanału nr 50 z lokalizacją przyznaną przez operatora. Dane także będą zapisywane do pliku z logami. Opcja ta działa tylko przy pracy w paśmie GSM, nie na każdej stacji bazowej.
- **CBS service number** – (działa na wszystkich telefonach z wyj. Symbian OS 9.x) - ustawiamy kanał nr **50**
- **Cell position from CBD** – tylko dla Symbian OS 9.x – funkcja i tak nie działa, zostawiamy **ON**
- **Beep on unknown Cell** – ustawiamy dźwięk zgodny z własnymi preferencjami
- **Beep on good Signal** – najlepiej ustawiamy na **NoSound** ze względu na fakt, iż aplikacja nie pozwala poprawne wyświetlanie poziomu sygnału – wina Nokia API
- **Beep Signal on .. dBm** – najlepiej nie zmieniamy (defaultowo **53**, czyli -53 dBm)

Konfiguracja dla menu Display jest następująca:

- **View Bar as** – pozostawiamy defaultowo **dBm**. Aplikacja nie pozwala poprawne wyświetlanie poziomu sygnału – wina Nokia API
- **Show short Cell Id** – ustawiamy na **Off**, dzięki czemu dla sieci UMTS/3G widoczny będzie dodatkowo numer RNC (Radio Network Controller)
- **Database Format –** ustawiamy **V. 3.0 dec** (ustawienie niezbędne do ściągnięcia bazy stacji bazowych do programu, patrz następna część tutoriala)
- **Import data as –** ustawiamy **UTF-8** (ustawienie niezbędne do ściągnięcia bazy stacji bazowych do programu, patrz następna część tutoriala)
- **Second Search –** zostawiamy defaultowe – **On**. Program wyszuka w bazie zewnętrznej stacje bazowe, które mają identyczny CellId i LAC. Jeśli nie znajdzie, baza zostanie przeszukana jeszcze raz, ale tylko po CellId
- **Refresh Seconds –** zostawiamy defaultowe – **2**
- **Light always on** – zostawiamy defaultowe – **Off**, chyba, że należy nam na stałym podświetlaniu wyświetlacza (działa, gdy bateria ma więcej niż 30% pojemności). Przy okazji należy zwiększyć czas do włączenia się wygaszacza wyświetlacza w odpowiednich ustawieniach telefonu

- **Receive GPS Data** (tylko dla Symbian OS 9.x)**:** program Celltrack umożliwia zbieranie logów wraz ze współrzędnymi GPS. W **Options** -> **Display** -> znajduje się dodatkowa opcja **Receive GPS Data**. Jeśli posiadamy wbudowany GPS możemy wybrać **intern**, jeśli korzystamy z GPS przez Bluetooth wybieramy **extern**. Po wybraniu opcji pobierania współrzędnych GPS, należy zrestartować aplikację. Korzystanie z urządzenia GPS może spowodować znaczne przyspieszenie wyczerpywania się baterii. Dla Symbian OS 9.x dodatkowo istnieją w pliku z logami dwie dodatkowe kolumny ze współrzędnymi GPS miejsca, w którym nastąpiło zalogowanie się do danego sektora.



18

Po poprawnej konfiguracji urządzenia GPS (i dograniu plików clf – szczegóły w następnej części tutoriala) w oknie Cell Loc (zdjęcie nr 18) powinniśmy otrzymać: aktualne współrzędne GPS (ostatnie dwie cyfry są zapisywane w formacie sekund dziesiętnych), prędkość ruchu, liczbę dostępnych satelitów oraz inne informacje. Większość urządzeń GPS generuje współrzędne zgodnie z WGS84, w innym przypadku program Celltrack może mieć problemy z właściwym wyświetlaniem współrzędnych.

Po poprawnej konfiguracji telefonu, program będzie spisywał logi, gdy telefon będzie zmieniał dany sektor stacji bazowej. Plik (pliki) z logami dostępne są w katalogu ?:\Nokia\Others\CellTrack pod nazwami tracexxxx.clf i zawierają następujące kolumny: **Data, Godzina, CellId, LAC, RNC, kod kraju, kod sieci, wsp. GPS Longtitude (dł. geograficzna), wsp. GPS Latitude (szer. geograficzna), poziom sygnału w %, poziom sygnalu w dBm, informacja z kanału CBS, nazwa z dograney bazy clf**. Dla wersji dla Symbian OS 7.0/8.0 nie ma dwóch kolumną związanych ze współrzędnymi GPS. W pliku z logami dla OS 9.x przykładowo otrzymamy (gdy włączony jest GPS):

20080726 184553 28397 27000 2301 260 03 50.089201 19.903757 100% -91 -
Krakow, ul. Conrada 51 - Impol

20080726 184613 28858 27000 2301 260 03 50.089440 19.905834 100% -91 -
Krakow, ul. Stawowa 140 – Karcher

W celu edycji istniejących już wpisów w bazie clf można wykorzystać**: Options- > Edit a cell** (o bazach clf więcej w następnej części tutoriala).

PyNetMony:

Konfigurację przeprowadzamy po wejściu **Options -> Settings 1** lub **Settings 2**. Konfiguracja dla menu **Settings 1** jest następująca:

- **Cellselection Notifier** – powiadomienie dźwiękowe o nowej stacji. Możliwe konfiguracje: OFF, Sound, Voice, Only new. Wybieramy **Only new** – powiadomienie o nowej stacji lub **OFF**.
- **Light** - zostawiamy defaultowe – **OFF**, chyba, że należy nam na stałym podświetlaniu wyświetlacza
- **WLAN Scan [s]...** – ustawiamy na **0**, nie zajmujemy się monitoringiem sieci WLAN
- **Volume** – głośność powiadomienia o nowej stacji, zostawiamy wartość **5**.
- **Voice Text** – używane w momencie wybrania opcji w **Cellselection Notifier -> Voice**. Informuje dźwiękowo o konkretnych parametrach stacji

- **GPS** – jeśli posiadamy urządzenie GPS ustawiamy albo **Internal** (wbudowany), **External** (po Bluetooth) lub **Assisted** (czyli wbudowany z dodatkową opcji użycia połączenia z Internetem w celu szybszego odczytania sygnału z satelitów powodując przyspieszenie wyliczenie położenia GPS terminala (GPS Fix))
- **Neighbour Radius [km]** – promień maksymalnego pomiaru w oknie Radar, wybieramy wartość np **3 km**
- **WLAN Autosave Interval [min] –** nie zajmujemy się monitoringiem sieci WLAN, nie zmieniamy nic
- **CLF stored on** - wybieramy miejsce, gdzie chcemy wrzucać pliki ze stacjami bazowymi (o wgrywaniu plików clf w następnej części tutoriala). Wybieramy np kartę pamięci czyli **Memory Card**
- **WLAN Database stored on** – nie zajmujemy się monitoringiem sieci WLAN, nie zmieniamy nic
- **WLAN Notifier** - nie zajmujemy się monitoringiem sieci WLAN, nie zmieniamy nic
- **Map Zoom Level (1-12)** – związane z dogrywaną mapką z google maps w oknie Map. Ustawiamy wartość wg. własnych preferencji.
- **Sec between BT Scans** - ustawiamy na **0**, nie zajmujemy się monitoringiem urządzeń Bluetooth
- **BT Database stored on -** nie zajmujemy się monitoringiem urządzeń Bluetooth, nie zmieniamy nic
- **BT Notifier --** nie zajmujemy się monitoringiem urządzeń Bluetooth, nie zmieniamy nic
- **BT Autosave Interval [min]-** nie zajmujemy się monitoringiem urządzeń Bluetooth, nie zmieniamy nic
- **BT Scan Timeout [s] -** nie zajmujemy się monitoringiem urządzeń Bluetooth, nie zmieniamy nic
- **CLF Autosave interval [min]** – ustawiamy co jaki czas mają być dogrywane logi do pliku (oprócz momentu przy wyłączaniu aplikacji), można ustawić np **15 min**
- **Color Theme** – ustawiamy wartość wg. własnych preferencji (**Blue**/Black/Red/Green/Magenta)
- **Font Size** – ustawiamy wartość wg. własnych preferencji (Small/**Medium**/Large/XL)

Po ustawieniu powyższych parametrów należy wejść do **Options -> Save** w celu zapisania ustawień

Konfiguracja dla menu **Settings 2** jest następująca:

- **WLAN Positioning System** – nie zajmujemy się monitoringiem sieci WLAN, nie zmieniamy nic
- **Radar Mode** – w oknie Radar mają pojawiać się informacje dot. stacji bazowych z plików clf, ustawiamy **CLF**
- **Geocache LAT** – brak danych o wpływie ustawień, najlepiej nie zmieniamy nic
- **Geocache LON** – brak danych o wpływie ustawień, najlepiej nie zmieniamy nic
- **WLAN Sorted by** – nie zajmujemy się monitoringiem sieci WLAN, nie zmieniamy nic
- **BSSID Notifier** – nie zajmujemy się monitoringiem sieci WLAN,nie zmieniamy nic
- **LAC Check for CLF search** – wybieramy **ON** – stacje będą szukane w bazie za pomocą LAC i CellId. W aktualnej wersji aplikacji brakuje opcji ponownego wyszukania tylko po CellId. Oznacza to, iż w przypadku zmiany LAC (co zdarza się bardzo często), stacja będzie traktowana jako nowa. Wybranie opcji **OFF** może spowodować błędy – CellId nie jest unikalny w skali kraju
- **GSM / 3G Log Event** - ustawiamy **Cellchange only** – wszystkie zmieniające się sektory stacji bazowych będą spisywane do plików z logami w miejscu wybranym w ustawieniach **Settings 1**
- **POS Upload Interval [min]** – co jaki okres czasu mają być wysyłane współrzędne do serwera producenta (do podglądnięcia na http://www.daniel-perna.de/pynetmony/map.php). Nie używamy tej opcji, więc zostawiamy defaultowe ustawienia

Po ustawieniu powyższych parametrów należy wejść do **Options -> Save** w celu zapisania ustawień

Dodatkowe ustawienia programu:

- w celu włączenia zbierania logów każdorazowo po włączeniu programu należy wybrać: **Options -> Start 2G/3G Logging**
- w celu włączenia urządzenia GPS należy każdorazowo po włączeniu programu wybrać: **Options -> Start GPS**

- inne opcje z menu Settings: Orientation (zmiana orientacji wyświetlacza), Voice Setup (ustawienia dot. powiadomienia dźwiękowego), Set Default APN (wybranie defaultowego APN do połączenia z internetem na potrzeby pobrania mapy google lub informacji dot. satelitów do wyliczenia współrzędnych GPS)
- opcja Database > Kismet Export – nieużywana – nie zajmujemy się monitoringiem sieci WLAN
- opcje Map -> pozwalają na podejrzenie poszczególnych parametrów: Cell (clf) Position , GPS Position, Google Position lub podesłanie do serwera producenta i podejrzenia lokalizacji na jego mapce: Upload Position (http://www.daniel-perna.de/pynetmony/map.php) czy pobranie współrzędnych: Get Google Coordinates

W celu dopisania lub edycji istniejących wpisów w bazie clf w telefonie można wykorzystać: **Options -> Database -> Edit a cell** i **Options- > Database -> Add a cell** (o bazach clf więcej w następnej części tutoriala).

Logi znajdują się katalogu: \data\Others\PyNetMony\logs (folder z logami w zależności od konfiguracji z poprzedniej części tutoriala znajduje sie albo na karcie MMC albo w pamięci telefonu). Logi zapisywane są po każdym uruchomieniu programu do nowego pliku.

Przykład logu z programu PyNetMony (z włączonym przez moment urządzeniem GPS):
Date (Y/M/D);Time (H:M:S);CID;LCID;LAC;MCC;MNC;RNC;RXL;LON;LAT;SPEED;DISTANCE
2009/01/28;14:17:56;25231;n/a;21068;260;1;n/a;-50;19.923690;50.047337;0.3;2.296
2009/01/28;14:19:17;62062;n/a;2022;260;6;n/a;-74;19.923672;50.047383;0.4;1.411
2009/01/28;14:26:27;25231;n/a;21068;260;1;n/a;-67;n/a;n/a;n/a;n/a
2009/01/28;14:26:38;34032;150832368;21068;260;1;2301;-114;n/a;n/a;n/a;n/a
2009/01/28;14:27:09;52552;150850888;21068;260;1;2301;-114;n/a;n/a;n/a;n/a
2009/01/28;14:27:33;2064;1378320;22;260;6;21;-95;n/a;n/a;n/a;n/a

VI. Wgrywanie baz stacji bazowych i ich monitoring

WGRYWANIE BAZ STACJI BAZOWYCH DO CELLTRACKA:

W celu poprawnego wgrania plików clf, w ustawienia programu Celltrack ustawiamy **Database Format -> V. 3.0 dec i Import data as -> UTF-8**

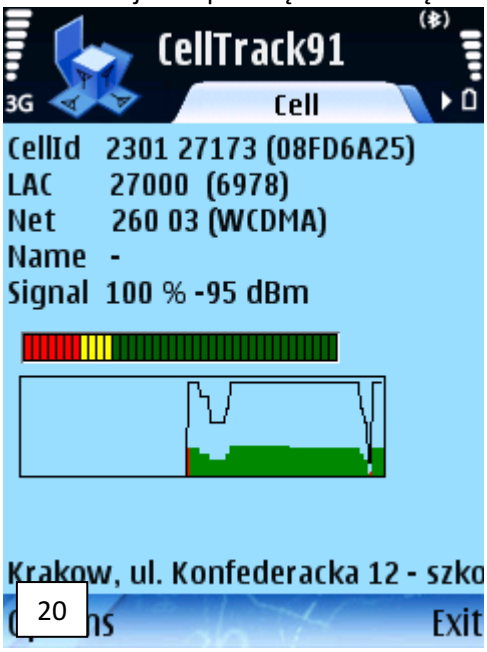
Pliki ze stacjami bazowymi najlepiej jest wrzucać w formacie 3.0, czyli: MCCMNC;CID;LAC;RNC;POS-LAT;POS-LON;POS-RAT;DESCRIPTION;RFU.
Przykładowo:
//cell list exchange format v3.0//
26001;21093;21015;00000;50.215;18.679167;0;Knurów, ul. Dworcowa 1 - komin;0

Takie pliki clf generujemy ze strony http://www.btsearch.pl/nobbimonitor.php wybierając odpowiednią sieć i województwa. Pliki clf zapisujemy z nazwą w formacie nr sieci np: 26001.clf dla Plusa. Dla tej sieci można generować także pliki clf wraz ze współrzędnymi GPS i numerami RNC.

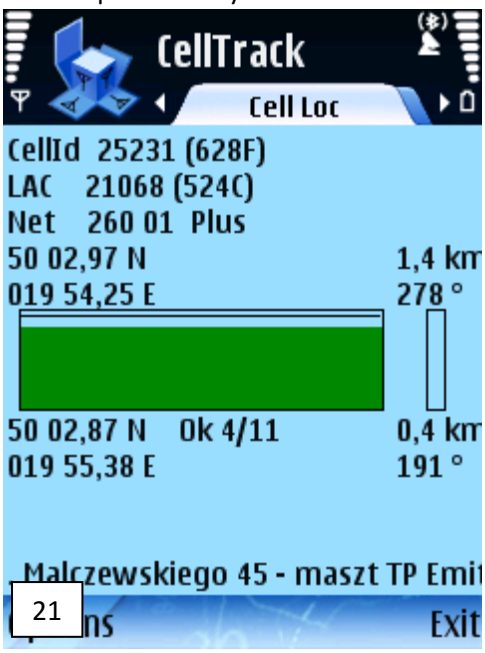
Pliki wrzucamy do katalogu z programem, tam gdzie znajdują się logi (plik trace). Po wrzuceniu plików do folderu programu wchodzimy do **Options** -> **Database** -> **Generate DB** (zdjęcie nr 19) generujemy ściągnięte pliki clf. Wgrywanie plików clf powtarzamy dla każdej z sieci. Trwa to bardzo szybko w porównaniu z plikami z wersji CLF 2.0 (także dostępne na stronie btsearch.pl). Po wgraniu plików, restartujemy program Celltrack. Poprawne wgranie plików clf powinno skutkować pojawieniem się lokalizacji stacji bazowej m.in. w głównym oknie – Cell (patrz zdjęcie nr 20), jeśli takowa została wpisana do bazy http://www.btsearch.pl. W pliku trace także zamiast pola **no info** pojawi się lokalizacja stacji.

W przypadku Celltrack dla Symbian OS w wersji 9.x po włączeniu urządzenia GPS powinniśmy w oknie Cell Loc zobaczyć oprócz naszej stacji, jej współrzędne GPS (pola nad wykresem na zdjęciu nr 21).
Bazy stacji bazowych najlepiej jest wrzucać po każdej jej aktualizacji, podmieniając odpowiednie pliki clf i włączając opcję generowania.

Jeśli wystąpią problemy przy generowaniu plików można spróbować wygenerować pliki clf v. 2.0 po wcześniejszym skonfigurowaniu opcji formatu clf w ustawieniach Celltracka. Problemy z aplikacją ma m.in. telefon Nokia N73.



20



21

WGRYWANIE BAZ STACJI BAZOWYCH DO PyNetMony:

W celu poprawnego wgrania plików clf wrzucamy jedynie pliki clf w wersji 3.0 dec. Takie pliki pliki clf generujemy ze strony http://www.btsearch.pl/nobbimonitor.php wybierając odpowiednią sieć i województwa. Dla sieci Plus można generować także pliki clf wraz ze współrzędnymi GPS i numerami RNC.
Pliki ze stacjami bazowymi najlepiej jest wrzucać w formacie 3.0, czyli: MCCMNC;CID;LAC;RNC;POS-LAT;POS-LON;POS-RAT;DESCRIPTION;RFU.
Przykładowo:
//cell list exchange format v3.0//
26001;21093;21015;00000;50.215;18.679167;0;Knurów, ul. Dworcowa 1 - komin;0

W stosunku do Celltrack niewymagane jest dodatkowe generowanie, jednak pliki wymagają innego nazywania np:
26001_gsm.clf lub 26003_umts.clf, czyli „nrsieci_pasmo.clf" - autor aplikacji proponuje oddzielenie plików clf dla różnych pasm. Formularz do plików clf ze strony www.btsearch.pl nie umożliwia generowania plików odróżniając pasma, ale nie ma wływu fakt, iż np plik 26001_gsm zawiera także stacje UMTS/3G. Oba pliki mogą mieć więc identyczne dane.

22

Pliki wrzucamy w zależności od konfiguracji z poprzedniej części do:

- folderu na karcie pamięci: \data\Others\PyNetMony\clf
- lub do folderu w pamięci telefonu: \data\others\PyNetMony\clf

Poprawne wgranie plików clf powinno skutkować pojawieniem się lokalizacji stacji bazowej m.in. w głównym oknie NetMon (przykład na zdjęciu nr 22), jeśli takowa została wpisana do bazy http://www.btsearch.pl. Bazy stacji bazowych najlepiej jest wrzucać po każdej jej aktualizacji, podmieniając odpowiednie pliki.

MONITORING PRZY UŻYCIU APLIKACJI:

W trakcie mijania danej stacji należy obserwować zmiany parametrów LAC / CID. Dane te mogą być spisywane do logów – po odpowiednich ustawieniach programów – patrz poprzednie części.

W celu dopisania lub edycji istniejących nazw (wpisów) w bazie clf można wykorzystać w PyNetMony: Options- > Database -> Edit a cell i Options- > Database -> Add a cell. W przypadku Celltracka: Options- > Edit a cell

Bardzo pomocne jest dogranie baz stacji bazowych ze strony www.btsearch.pl. Jeśli pojawi się stacja, której nie ma na http://www.btsearch.pl, oprócz informacji dźwiękowych, w logach (pliki trace) dla Celltracka powinniśmy otrzymać:

20081029 185418 28449 27000 2301 260 03 0.000000 0.000000 100% -95 - no info (WCDMA)

Jak widać powyżej dla wpisów stacji UMTS/3G mamy dodatkowo wartości RNC oraz dopisane na końcu „(WCDMA)” Następujące logi:

20081028 084604 21058 20409 2501 260 03 0.000000 0.000000 100% -87 - *:Chorzow, Batory - komin ul. Czempiela 54
20081028 084828 58938 20409 2501 260 03 0.000000 0.000000 29% -111 - *:[???] Swietochlowice ?, ?

oznaczają, iż obie stacje zmieniły LAC lub istnieje jakaś nowa stacja (przed nazwą jest „***:**”), zaś w przypadku drugiej stacji dodatkowo sektor stacji nie był potwierdzony w bazie na http://www.btsearch.pl – w polu końcówki dla tego CellId jest „?”. W logach widoczne jest to po „**[???]**” w ostatniej kolumnie przez lokalizacją z bazy clf.

W logach PyNetMony (w porównaniu do Celltracka) niestety nie jesteśmy w stanie podejrzeć nazwy stacji oraz informacji i niepasującym LAC w stosunku do wersji z bazy btsearch. Fragment logu z programu PyNetMony (z włączonym urządzeniem GPS):

Date (Y/M/D);Time (H:M:S);CID;LCID;LAC;MCC;MNC;RNC;RXL;LON;LAT;SPEED;DISTANCE
2009/01/28;14:17:56;25231;n/a;21068;260;1;n/a;-50;19.923690;50.047337;0.3;2.296
2009/01/28;14:19:17;62062;n/a;2022;260;6;n/a;-74;19.923672;50.047383;0.4;1.411
2009/01/28;14:26:27;25231;n/a;21068;260;1;n/a;-67;n/a;n/a;n/a;n/a
2009/01/28;14:26:38;34032;150832368;21068;260;1;2301;-114;n/a;n/a;n/a;n/a
2009/01/28;14:27:09;52552;150850888;21068;260;1;2301;-114;n/a;n/a;n/a;n/a
2009/01/28;14:27:33;2064;1378320;22;260;6;21;-95;n/a;n/a;n/a;n/a

W przypadku dużego pliku z logami należy skopiować go na dysk twardy komputera i usunąć z pamięci telefonu komórkowego. Programy automatycznie stworzą nowe pliki trace.

INFORMACJE KOŃCOWE:

W celu porównania plików z logami z bazą aktualną bazą http://www.btsearch.pl, można wykorzystać skrypt AnaLOGyzer dostępny na http://www.btsearch.pl/analogyzer.php. Logi oraz inne informacje dot. stacji bazowych prosimy nadsyłać także na nowe@btsearch.pl lub btsearch@btsearch.pl

Zapraszamy do współpracy !

VII. Kontakt

W przypadku znalezienia błędów, pytań oraz oczekiwań wobec nowych wersji tutoriala proszę o kontakt na adres mailowy:

k.niemczyk@btsearch.pl

W przypadku podsyłania nowości, logów oraz pytań o stacje bazowe:

nowe@btsearch.pl lub btsearch@btsearch.pl

Podziękowania dla Dawida Lorenza za pomoc w przygotowaniu tutoriala.

VIII. Ostatnie zmiany w tutorialu

Wersja	Ostatnia modyfikacja	Zmiany
1.07	2011-08-09	Nośne i nazwa sieci Era->T-Mobile
1.06	2010.01.23	Drobne poprawki i uzupełnienia, poprawki nośnych
1.05	2009.06.13	Drobne poprawki i uzupełnienia
1.04	2009.04.21	Drobne poprawki i uzupełnienia
1.03	2009.02.18	Drobne poprawki i uzupełnienia
1.02	2009.02.13	Drobne poprawki i wyjaśnienia
1.01	2009.02.11	Drobne poprawki techniczne

1.00	2009.02.10	Wersja początkowa