



EGI Security

ELECTRONIC INTELLIGENCE

GSM INTERCEPTION

Cellular Network Monitoring System

GSM INTERCEPTION

Destination: is applied for searching, intercepting and signal recording of cellular networks with the purpose of control of talks, SMS and localization of subscribers.

The complex is soft-hardware and consists of:

The hardware:

- The unit of signals' receiving and processing - up to 8 units on 1 control computer (up to 128 channels).
- Antenna-feeder system.
- The control computer (Notebook).



The software:

- **The control program for units of signals' receiving and processing.**
- **Applications for processing archives.**
- **Decoder A5/2 - as an integration option of the control computer.**

Technical capabilities:

- **Interception and decoding of signals from base stations and mobile telephones GSM frequency band 850/900/1800/1900 Mhz in real time.**

- The cellular networks' control with hopping application.
- An automatic recording of negotiations and the protocol on a disc or the external carrier.
- Voice codecs FR, EFR, HR.
- SMS the decoder for national alphabets and UNICODE.
- Archives, such as «sound + events» with partitioning on dates and on subscribers.
- The channels restoration system for reduction of probability of the purpose's skip at the intensive traffic.
- The "pilot" call for detection of the subscriber and his numbers.
- Developed system of events filters of the cellular network.
- Interactive general and channel events protocols with system of filters.

System Components:

- **Hardware**
- **Antennas and feeders set**
- **Connecting Cable to Be Connected to the PC's USB-port**
- **Power Cable**
- **Car Lighter Connecting Cable**
- **CD, Containing Software**
- **CD, Containing Operating Instruction**
- **Test Mobile Phone with the Open Engineering Program**
- **“Boomerang” Device for IMSI and TMSI Determination**
- **IKG Head phones**
- **Portable Computer**

Basic Program of the System

GM_v3.19 XP Edition

File Sets Tracking mode Windows Tools Help

RAND IMSI DIST NUM REV IMEI TYPE KEY

Receivers

Nº	Cell	Mode	RX level (dBm)	State
1	10/1		-71	T:810740CE
2	7/7		-59	T:810734BE
3	120/1		-72	T:81074619
4	688/0		-86	UK VODAFONE
5	34/0		-61	T:8107308D
6	817/3		-68	T:81074FD3

Recorder

Nº	Cell	Mode	RX level (dBm)	Time	State
1					
2	7		T:810734BE	01:38	
3	01		T:81074619	00:48	
4	52				
5			T:8107308D	01:44	
6	30		T:81074FD3	00:25	

Codec: PCM; Parameters: 8 000HZ; 16 bit; Mono

Target list

Name	PLMN number	CL500	CL1800	IMSI	TMSI	IMEI	KEY
Mikkey...	242-0423444	Y	Y	N	N	N	N
Lapout	4924425	Y	Y	Y	unk	Y	Y
betyr	234-4-23-4...	Y	Y	Y	unk	Y	N

Total phones: 3 Last Event: Unknown

Protocol

General Rec 1 Rec 2 Rec 3 Rec 4 Rec 5 Rec 6 Rec 7 Rec 8

```

R6: Release channel: conditional IE error
R6: Paging response TMSI=7307400E CL1800-301803 11:39:
R6: Authentication request
R1: Paging response TMSI=730740C56 CL900-331881 11:39:5
R6: Cell Identity: ID=1234,LAC=009
R1: Cell Identity: ID=2345,LAC=009
R1: Authentication request
R6: Start ciphering: no ciphering
R6: TMSI Reallocation TMSI=81074FD3
R1: Start ciphering: no ciphering
R6: Call
R6: Assignment into 817/3
R6: SMS from 555-0123: 'Let load the oranges in a barrel
R1: Paging response TMSI=8107308A2 CL900-331981 11:40:0
R1: Cell Identity: ID=2345,LAC=009
R1: Authentication request
R6: Connect acknowledge
R1: Start ciphering: no ciphering
R1: Paging response IMSI=234016739034777 CL900-335981
R1: Authentication request
R1: Cell Identity: ID=2345,LAC=009
R1: Start ciphering: no ciphering
R1: TMSI Reallocation TMSI=8107336C
R1: Call from 8-902-6345203
R1: Assignment into 10/5
R1: Cell Identity: ID=2345,LAC=009
R4: Call establishment TMSI=CF987406 CL1800-301881 11:
R4: Authentication request
R4: Start ciphering: no ciphering
R1: Connect acknowledge
R1: Disconnect Normal call clearing
R1: Release complete Normal call clearing
R1: Release channel: normal release
R1: Call establishment TMSI=730740CE CL900-331881 11:4
R1: Authentication request
R1: Cell Identity: ID=2345,LAC=009
R1: Start ciphering: no ciphering
    
```

Working Area of the Basic Program is divided into four main parts:

- **Top left-hand third is a window of receivers' current status (Receivers Window);**
- **Middle left-hand third is a window of voice data recording channels current status (Recorder Window);**
- **Bottom left-hand third is a window of intercepted numbers list, their selection parameters and their current status (Target List Window);**
- **Right-hand half is a protocol window that is registering events in received channels (Protocol Window).**

GM_4.05 XP Edition

File Sets Trading mode Windows Tools Help

RAND IMSI DIST NUM REV IMEI TYPE KEY

Receivers

1	Cell	Mode	Rx level (dBm)	State
1	103/5		-35 -35	T:6E6298BF

Recorder

1 85 T:6E6298BF 00:07

Codec: PCM; Parameters: 8,000 kHz, 16 Bit, Mono

Cell list

Cell list (C:\Program Files\GMV4_05\Graphics_Soft\cell)

Name	Provider	LAC	ID	BCH	RxLev (dBm)	Do
Cell	BG-05	1500	20552	103	-36	
Cell	BG-05	1500	20561	115	-48	
Cell	BG-05	1500	20551	113	-56	
Cell	CITRON BG	7700	7996	34	-38	
Cell	CITRON BG	7700	7950	66	-50	
Cell	CITRON BG	7700	7934	42	-70	
Cell	YU MOBEL	1800	8003	54	-63	
Cell	YU-03	56010	12902	61	-56	
Cell	YU-03	56010	22902	58	-63	

Protocol

General Rec1

```

R1: Cell Identity: ID=20552,LAC=1500,BG-05
R1: Authentication request
R1: Start ciphering: A5/1
R1: Paging response TMSI=55E4314P CL900=331985 KCH=0 31/10/04 10:40:43
R1: Cell Identity: ID=20552,LAC=1500,BG-05
R1: Authentication request
R1: Start ciphering: no ciphering
R1: Identity Request
R1: Setup: call from Anonymous
R1: Assignment into 103/6
R1: Cell Identity: ID=20552,LAC=1500,BG-05
R1: Connect acknowledge
R1: Disconnect Normal event, unspecified
R1: Release complete Normal event, unspecified
R1: Release channel: normal release
R1: Paging response TMSI=55E4314P CL900=331985 KCH=1 31/10/04 10:41:01
R1: Authentication request
R1: Cell Identity: ID=20552,LAC=1500,BG-05
R1: Start ciphering: no ciphering
R1: Identity Request
R1: Release channel: normal release
R1: Call establishment TMSI=46E73BC0 CL900=331981 KCH=0 31/10/04 10:41:10
R1: Cell Identity: ID=20552,LAC=1500,BG-05
R1: Start ciphering: A5/1
R1: Call establishment TMSI=5D566155 CL900=331981 KCH=4 31/10/04 10:41:22
R1: Start ciphering: A5/1
R1: Call establishment TMSI=5D566155 CL900=331981 KCH=4 31/10/04 10:41:47
R1: Cell Identity: ID=20552,LAC=1500,BG-05
R1: Start ciphering: A5/1
R1: Paging response TMSI=6EA20B94 CL900=331985 KCH=4 31/10/04 10:41:52
R1: Cell Identity: ID=20552,LAC=1500,BG-05
R1: Authentication request
R1: Start ciphering: no ciphering
R1: Identity Request
R1: SMS from 088-7337391 original SC +3-598-9100000 Short message received by SME
R1: Release channel: normal release
R1: Call establishment TMSI=46E73BC0 CL900=331981 KCH=0 31/10/04 10:41:58
R1: Start ciphering: A5/1
R1: Call establishment TMSI=6E6298BF CL900=331981 KCH=0 31/10/04 10:42:14
R1: Authentication request
R1: Cell Identity: ID=20552,LAC=1500,BG-05
R1: Authentication response
R1: Start ciphering: no ciphering
R1: Ciphering mode complete
R1: Identity Request
R1: Setup: dialling number 123
R1: Identity response IMEI=353795000446040
R1: Call proceeding
R1: Assignment into 103/5
R1: Assignment complete
R1: Alerting
R1: Connect with Unavailable
R1: Connect acknowledge
R1: Cell Identity: ID=20552,LAC=1500,BG-05
  
```

Protocol Windows

```
Protocol
Gen2B Rec 1 Rec 2 Rec 3 Rec 4 Rec 5 Rec 6 Rec 7 Rec 8
MO: Release channel: conditional IE error
MS: Paging response IMSI=7987488E CL1800=301885 11:39:56 21.01.03
MO: Authentication request
MS: Paging response IMSI=79874C56 CL900=331881 11:39:57 21.01.03
MO: Cell Identity: ID=1234,LAC=009
MS: Cell Identity: ID=2345,LAC=009
MS: Authentication request
MS: Start ciphering: no ciphering
MO: IMSI Reallocation IMSI=0107AF03
MS: Start ciphering: no ciphering
MO: Call
MS: Assignment into B17/3
MO: SMS from 555-0123: *Let load the oranges in a barrel.Money-at morning
MS: Paging response IMSI=818738A2 CL900=331981 11:40:03 21.01.03
MS: Cell Identity: ID=2345,LAC=009
MS: Authentication request
MO: Connect acknowledge
MS: Start ciphering: no ciphering
MS: Paging response IMSI=23401073903A777 CL900=333981 11:40:07 21.01.03
MS: Authentication request
MS: Cell Identity: ID=2345,LAC=009
MS: Start ciphering: no ciphering
MS: IMSI Reallocation IMSI=0107336C
MS: Call from 8-902-6345203
MS: Assignment into 19/3
MS: Cell Identity: ID=2345,LAC=009
MS: Call establishment IMSI=CF987406 CL1800=301881 11:40:12 21.01.03
MS: Authentication request
MS: Start ciphering: no ciphering
MS: Connect acknowledge
MS: Disconnect Normal call clearing
MS: Release complete Normal call clearing
MS: Release channel: normal release
MS: Call establishment IMSI=7307ABCE CL900=331881 11:40:26 21.01.03
MS: Authentication request
MS: Cell Identity: ID=2345,LAC=009
MS: Start ciphering: no ciphering
```





Purpose of Protocol Windows

Protocol Windows register all the System's activity. All the messages, concerning cellular system intercepted events, receivers' re-assignment, receiver's assignment to new radio channels, recording channels turning on and off and so on are displayed on the control PC screen. The above is done to provide for System's operator quick feedback as well as for saving operation protocol in a file for subsequent analysis of the working session.









Protocol Window has several tabs.

The one on the left (GENERAL) is a General Protocol Window. It displays the data coming from all of the receivers. Protocol Window is meant for displaying some groups of events both on the screen and in the protocol file as well as for ensuring quick access to the events processing commands.







ARCHIVE OF RECORDS Program


 **Archive of records**   

Commands Break sequence

File name	Changed	Time	Size
O_T#9446505B_1.wav	05.06.12 07:13	4.50	72046
O_T#94465D69_1.wav	05.06.12 07:14	23.50	376046
I_T#9446703B_1.wav	05.06.12 07:14	9.00	144046
I_T#94467AF7_1.wav	05.06.12 07:14	16.50	264046
O_T#94467F8B_1.wav	05.06.12 07:14	5.00	80046
I_T#9446970D_1.wav	05.06.12 07:15	25.00	400046
O_T#9446772E_1.wav	05.06.12 07:16	45.00	720046

 F:\
 Program Files
 GM
 DISTRIBUTION
 05 июн 2012
 **Random**

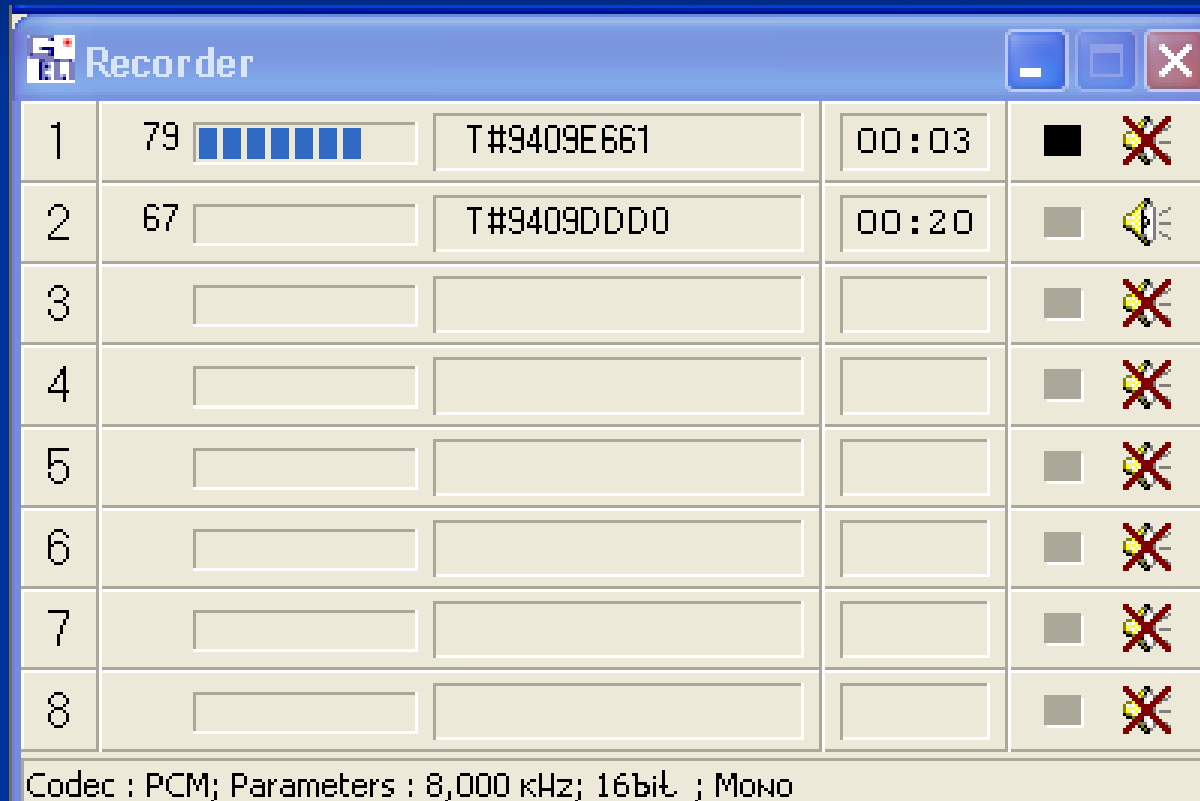
 f: [work2]

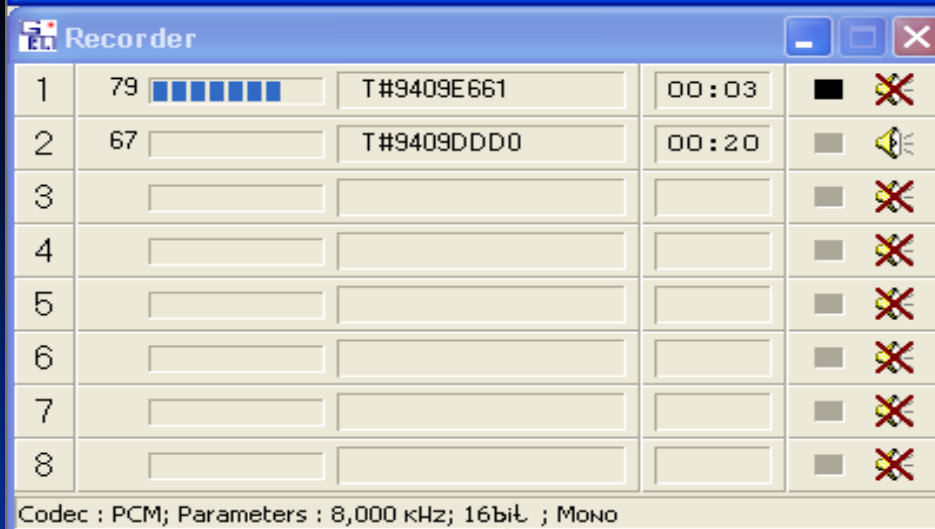
Files count 7

R4: Call establishment TMSI=9446510A CL1800=301885 KCN=6
R4: Authentication request
R4: Start ciphering: no ciphering
R4: TMSI Reallocation TMSI=94465D69
R4: Call proceeding
R4: Facility
R4: Assignment into 849/3

ARCHIVE OF RECORDS Program

Used for listening to and sorting speech files,
stored by the Basic Program.



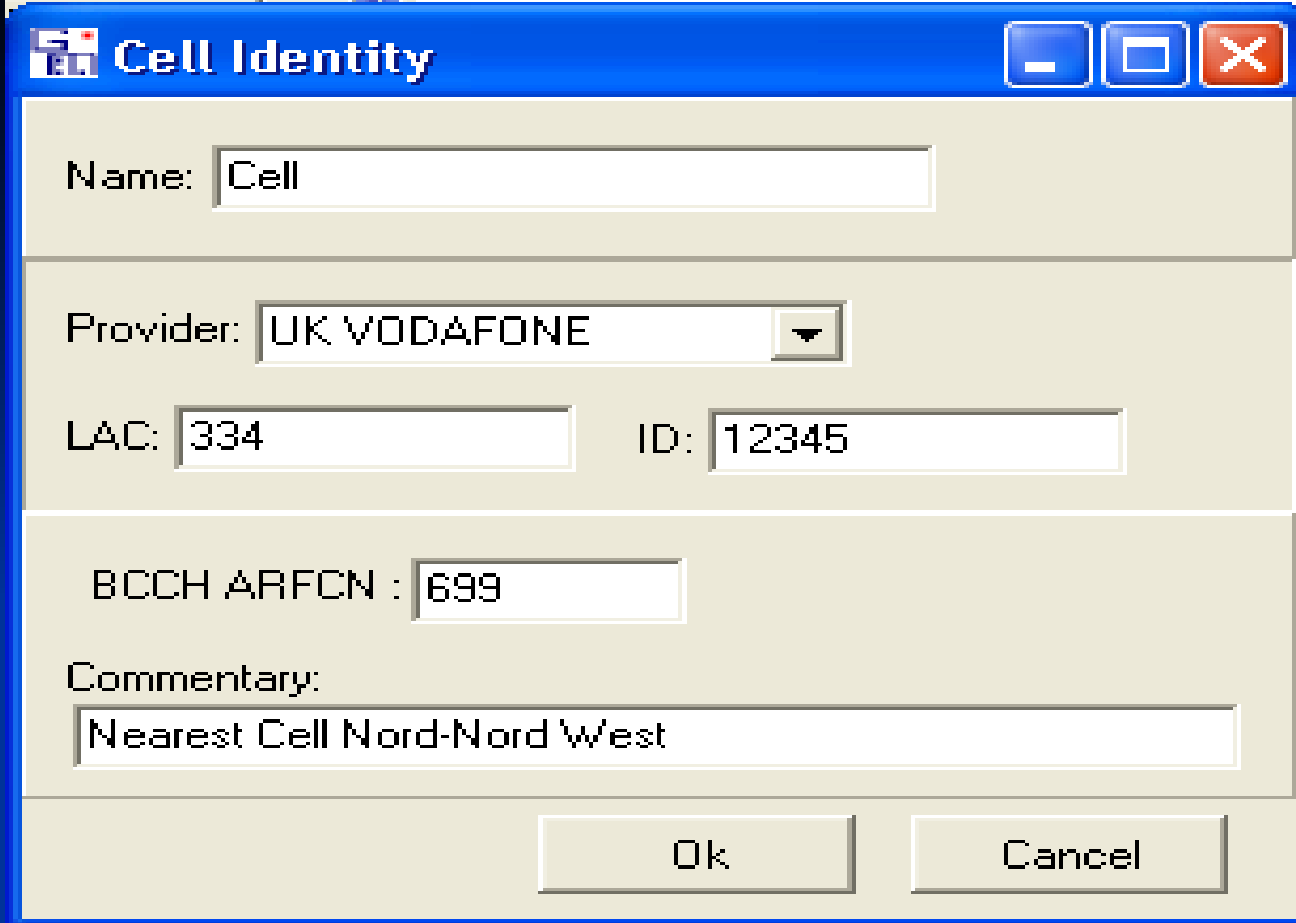


Sound Processing Window.

Purpose of Sound Processing Window:

Sound Processing Window is meant for solving software tasks of voice data recording and processing. Per se, Sound Processing Window is a software supported multichannel sound recorder.

The window supports standard functions of beginning and completion of sound recording, pausing as well as concurrent recording of all available voice channels and listening to one of the channels in real time. Each voice channel is connected to sound receiving unit.

A screenshot of a 'Cell Identity' dialog box. The dialog has a blue title bar with standard Windows window controls (minimize, maximize, close). The main area is light beige and contains several input fields. The 'Name' field contains 'Cell'. The 'Provider' field is a dropdown menu showing 'UK VODAFONE'. The 'LAC' field contains '334' and the 'ID' field contains '12345'. The 'BCCH ARFCN' field contains '699'. Below these is a 'Commentary' section with a text area containing 'Nearest Cell Nord-Nord West'. At the bottom are 'Ok' and 'Cancel' buttons.

Cell Identity

Name:

Provider:

LAC: ID:

BCCH ARFCN :

Commentary:

Base Station Parameters Edit Dialog.

Base Stations Description Dialog is meant for either entering or editing data, reflecting Base Stations parameters.

SMS Interception.

Text messages (SMS) when intercepted are stored as a text in a protocol file.

Decoder A5/2

For activity of the decoder A5/2 no preliminary identification information (for example, key K_i) is required. All necessary data for decoder's activity are intercepted during communication session.

It allows to hold interception of communication sessions with cryptographic protection A5/2 in real time mode.

The probability of successful deciphering of a session depends on quality of the intercepted signal.

On reliably received channels it reaches 100 %.

System's Technical Data

The technical data on receiving channel refers to the receiver input.

Parameter's name	GSM-900	DCS - 1800	PCS-1900	GSM-850
Forward Channel Received Frequencies Band, MHz	935-960 MHz	1805-1880	1930-1990	824-849
Reverse Channel Received Frequencies Band and Transmission in Active Mode, MHz	890-915 MHz	1710-1785	1850-1910	869-894
Frequency Channel Spacing	200 KHz			
The number of controlled channels, MHz	124	375	299	124

Receiver Type	With dual frequency conversion, asynchronous	With triple frequency conversion, asynchronous
Receiver sensitivity in Normal Environment (noise level=20dB)	Not worse than -105 dBm Level-wise BER=10 ⁻⁷	
Output Power	+30dBm	
Antenna Feed Impedance (within the working Frequencies Band)	50 Om	
Emitted interferences level	-36 dBm up to 1 GHz, (<-30 dBm > 1 GHz)	
Time of Hopping Step Change	<500μS	

Demodulator	GMSK Asynchronous (Ageree Systems Inc.)
Synchronization	Adaptive test
Air Frames Errors Correction	Viterby Convolution decoder, double strike
Consumed Wattage (per channel)	<1W
Speech Codecs	FR, EFR, HR
Combined Structure of Channels Organization	TDMA/FDMA
Range of Working Temperatures at not more than 90%	+5°C ...+40°C (it is possible to operate the system in the range of -20°C +50°C on condition there is no moisture of condensation, but in that case radio channel parameters can degrade and won't meet the ones specified in the Table)