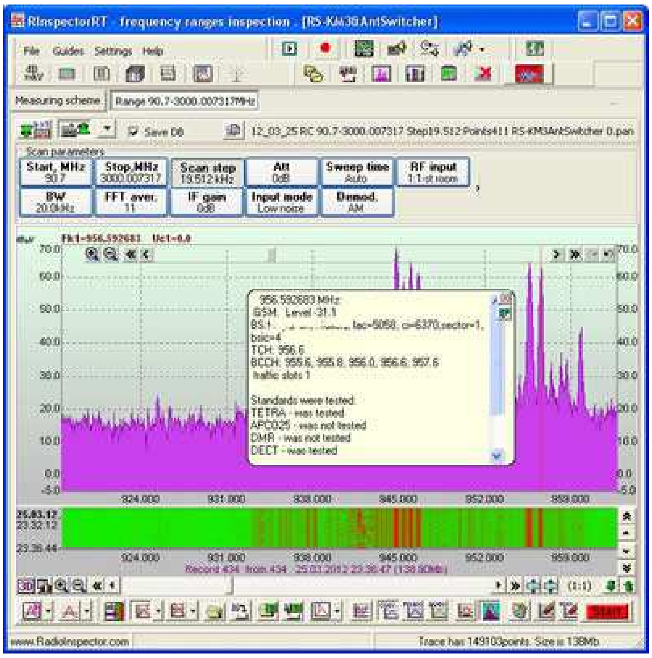
! "
$ %&& ' ("

! !) * + , -
(.
" ! !) * +
!) * + .
, !) * +

! +) + , * * . / * . * * +
+) + , 0 ! 1 0
0 ! 1 0 %
, 0 ! 1 0 ! 1 +) + ,
"
, +) + ,

GSM

The GSM demodulator derives the MCC, MNC, LAC, CI, and sector information. In addition, the TCH data channels that are linked to the analyzed BCCH channel and neighbouring BCCH channels can be received. Knowledge of these parameters allows the operator to determine the topology of GSM networks (GSM450, GSM850, GSM900, GSM1800, GSM1900). Illegal GSM base stations and GSM bugging devices can then be determined.



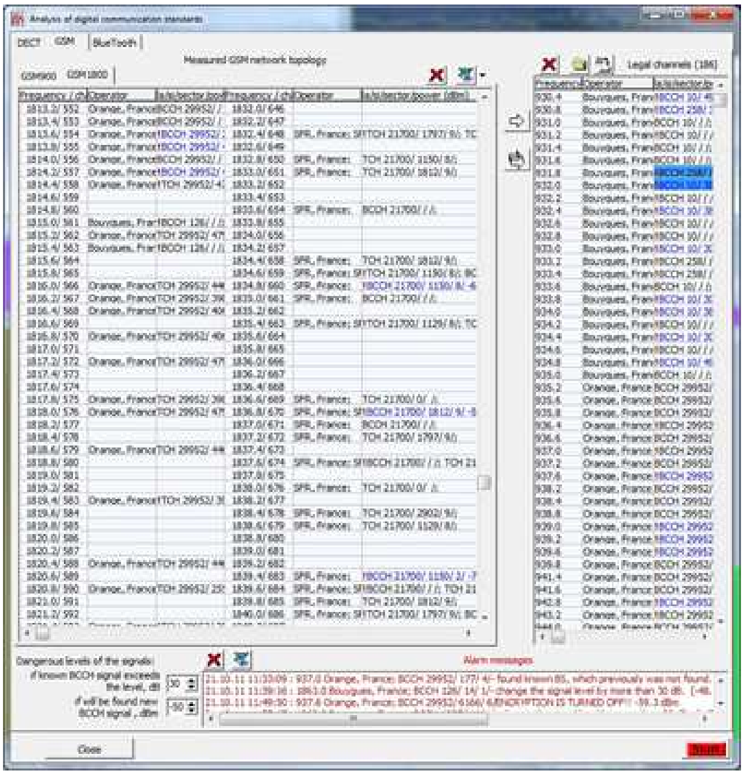
Start, MHz: 90.7
Stop,MHz: 3000.007317
Scan step: 19.512 kHz
Att: 0dB
Sweep time: Auto
RF input: 1:1-st room
BW: 20.0kHz
FFT aver.: 11
IF gain: 0dB
Input mode: Low noise
Demod.: AM

956.592683 MHz
GSM. Level -31.1
BS:1 [redacted] lac=5060, ci=6370,sector=1,
bsic=4
TCH: 956.6
BCCH: 955.6, 955.8, 956.0, 956.6, 957.6
traffic slots 1

Standards were tested:
TETRA - was tested
APCO25 - was not tested
DMR - was not tested
DECT - was tested

Figure 3. Signal analysis (GSM standard)

RadioInspector’s GSM signal analysis allows identification of "substituted" base stations which can be used in the interception of GSM traffic. RadioInspector does not perform voice demodulation of GSM standard.



Dangerous levels of the signals:
if known BCCH signal exceeds the level, dB: 30
if will be found new BCCH signal, dBm: -50

Alarm messages
21.10.11 11:33:09 : 937.0 Orange, France; BCCH 29952/ 177/ 4/- found known BS, which previously was not found.
21.10.11 11:39:16 : 1861.0 Bouygues, France; BCCH 126/ 14/ 1/- change the signal level by more than 30 dB. [-48.
21.10.11 11:49:30 : 937.6 Orange, France; BCCH 29952/ 6166/ 6/ENCRYPTION IS TURNED OFF!! -59.3 dBm

Figure 4. GSM network topology analysis

BlueTooth

The BlueTooth signal demodulator determines the addresses (LAP addresses) of BlueTooth devices which are switched on and in an active state (BlueTooth devices operating in the beacon mode - that is, periodically broadcasting beacon data), or operating BlueTooth devices. An estimation of transmitted traffic is displayed. From the evaluation of transmitted data, It can be determined if voice, burst data or file transmissions are occurring. A List of Authorized LAP addresses can be used to identify any new BlueTooth transmitter such as a BlueTooth keystroke logger,operating in a controlled premise. Received signal levels can be used to search for a BlueTooth transmitter with a given LAP address.

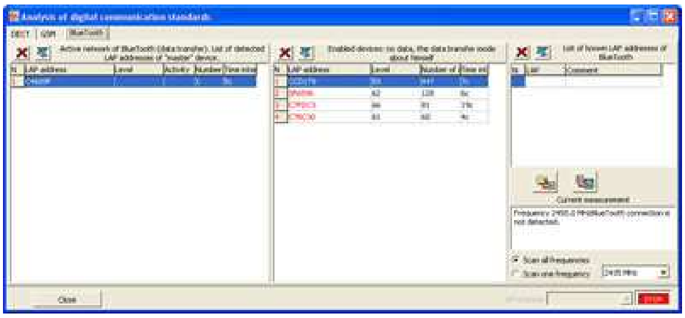
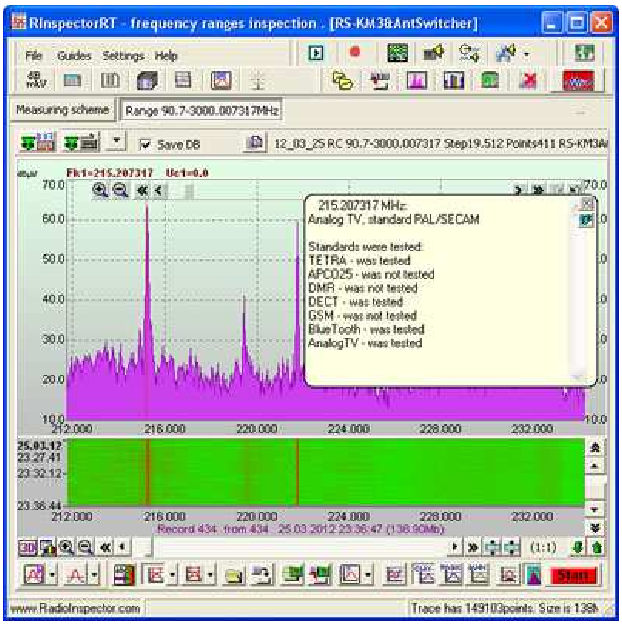


Figure 5. Signal analysis (BlueTooth standard)

Analog television PAL/SECAM/NTSC

The TV demodulator classifies TV Signals. The operator simply places a curser onto the TV signal frequency identified by RadioInspector, and the demodulated video is displayed in a separate pop-up window.



215.207317 MHz
Analog TV, standard PAL/SECAM

Standards were tested:
TETRA - was tested
APCO25 - was not tested
DMR - was not tested
DECT - was tested
GSM - was not tested
BlueTooth - was tested
AnalogTV - was tested

Figure 6. Radiation analysis (Analog TV)

When demodulating a TV signal RadioInspector defines the correct TV standard and synchronizes video accordingly. At low signal/noise ratios, if the program cannot synchronize the image and if video coding is in use, manual synchronization of lines and video frames can be used to provide a better display.

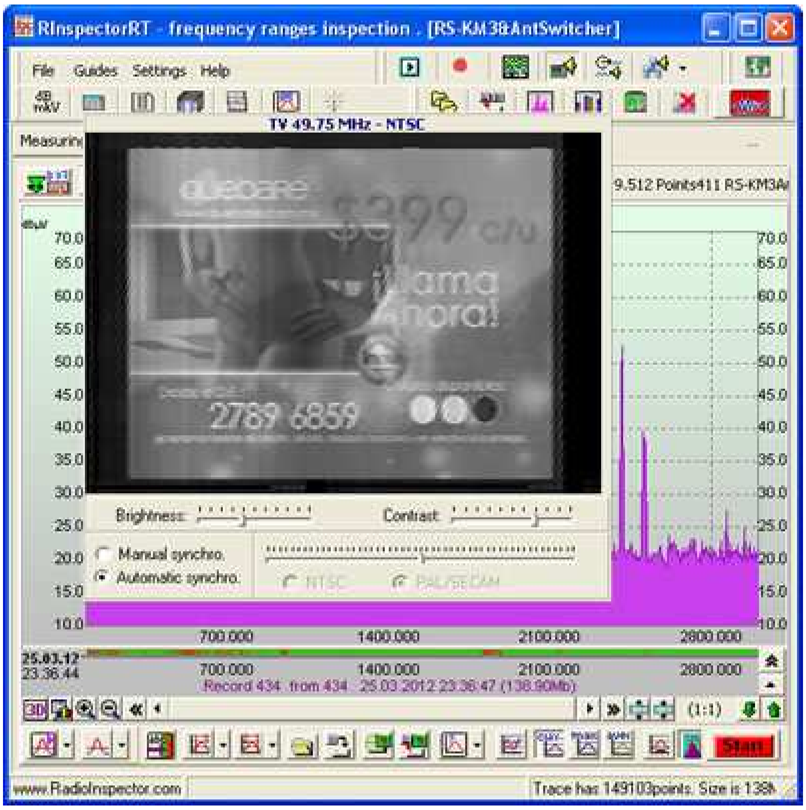


Figure 7. Video frame (Analogue TV)

APCO25

The APCO25 demodulator allows classifying APCO25 signals, displaying the source and destination addresses of messages; determining the network ID and demodulating voice if encryption is not used.

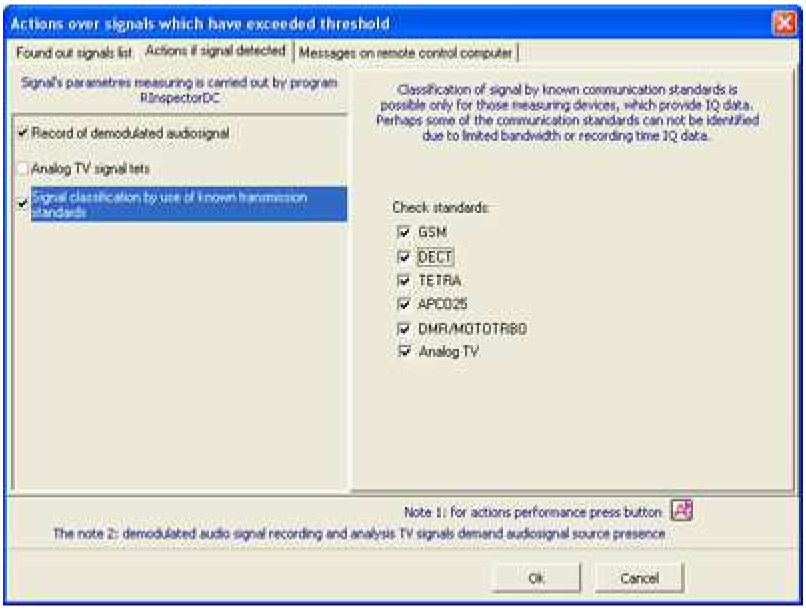
Figure 8. Signal analysis and voice demodulation (APCO25 standard)

DMR/MOTOTRBO

The DMR demodulator allows classifying DMR signals. The operator simply places a cursor onto the DMR signal frequency identified by RadioInspector, and the network ID source and destination addresses of messages are displayed in a separate pop-up window. Demodulation of voice is possible if encryption is not used.

Figure 9. Signal analysis and voice demodulation (DMR standard)

For ease of use of RadioInspector's "DTest" option, a special software utility was created to automatically 'identify while scanning' signals that exceed an operator defined RF signal level threshold line. This utility is used to automatically identify the DECT, BlueTooth, GSM, TETRA, APCO25, DMR and Analogue TV communication waveforms. The operator simply selects "Signal Classification of Common Signals" and a list of identified and classified signals is created automatically while scanning the radio frequency spectrum.



Signal's parametres measuring is carried out by program RInspectorDC

☑ Record of demodulated audiosignal

☐ Analog TV signal tets

☑ Signal classification by use of known transmission standards

Classification of signal by known communication standards is possible only for those measuring devices, which provide IQ data. Perhaps some of the communication standards can not be identified due to limited bandwidth or recording time IQ data.

Check standards:

☑ GSM
☑ DECT
☑ TETRA
☑ APCO25
☑ DMR/MOTOTRBO
☑ Analog TV

Note 1: for actions performance press button

The note 2: demodulated audio signal recording and analysis TV signals demand audiosignal source presence

Figure 10. Software utility for signal analysis of communication standards

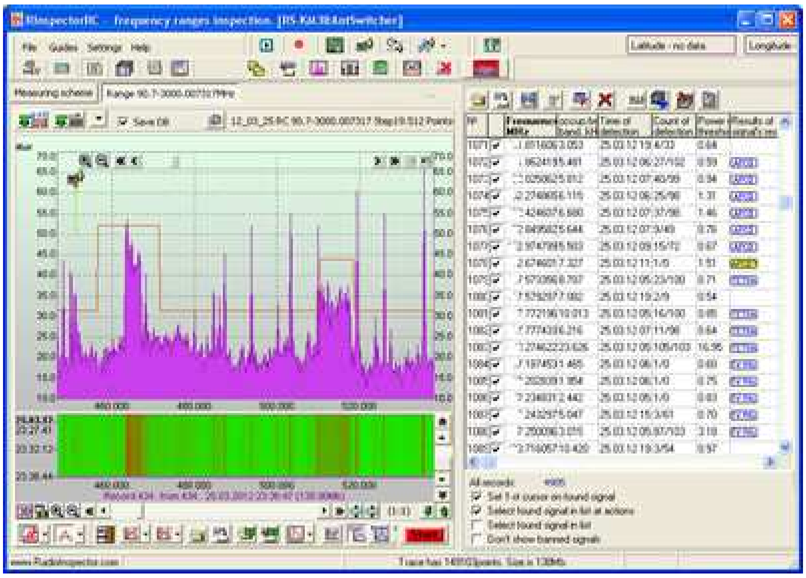


Figure 11. Results for automatic signal analysis and classification

We would be pleased to work with all manufacturers of receivers and spectrum analyzers whose instruments provide a continuous stream of IQ data or an IQ ability to read blocks of 1 second in the frequency band from 500 kHz to integrate these instruments into "RadioInspector".