"A unique product, there is no analogue or digital equivalent in the world! Digital analysis of radio frequency signal content! Automatic signal classification and recognition! Identification of digital communications transmitters by their addresses and other parameters.

RADIOINSPECTOR'S OPTIONAL DIGITAL SIGNALS ANALYSIS FEATURE "DTEST"

Realizing that further development of radio monitoring devices should include analysis and automatic classification of known communications standards, "RadioInspector" software engineers have developed a digital signal analysis option - "DTEST" ("Digital Test"). This option is designed for digital (software) demodulation of the most common communication standards and signals classification in accordance with these standards. This option is very simple to use: you should set the cursor on the signal you want to explore and push the button  . The program tunes the instrument to the cursor's frequency, receives necessary data and performs IQ signal demodulation for a given communication standard. The result of demodulation and signal classification is displayed on the screen.

DTest uses an array or a stream of IQ data transmitted by the instrument. The current version of RadioInspector's "DTest" option implements demodulators for the following communication standards:

- AM and FM analogue signals;
- DECT;
- TETRA;
- GSM;
- BlueTooth;
- Analog TV signal PAL / SECAM / NTSC (displays video);
- APCO25 (voice demodulation);
- DRM/MOTOTRBO (voice demodulation).
- ZigBee (802.15.4)

Compliance Table of the devices' capabilities connected to the "RadioInspector" software with digital analysis and streaming demodulation of digital signals (DTEST) option (the possibilities for identification, classification and demodulation depending on IQ bandwidth, IQ length and possibility of streaming of IQ)

	APCO25: radiation identification, transmitters classification	TETRA: radiation identification, transmitters classification	DMR/MOTOTRBO: radiation identification, transmitters classification	DRM: radiation identification	DECT: radiation identification, transmitters classification	BlueTooth: radiation identification, transmitters classification	GSM: radiation identification, transmitters classification, network topology discovery	ZigBee: radiation identification, transmitters classification	Analog TV (NTSC/PAL/SECAM): radiation identification	DVB-T: radiation identification	demodulation (voice) of APCO25	demodulation (voice) of TETRA	demodulation (voice) of DRM/MOTOTRBO	display analogue TV (NTSC/PAL/SECAM) video stream (without sound)	demodulation (voice) of DRM
Rohde&Shwarz FSL	+	+	+		+	+	+		+	-	-	-	-	-	
Rohde&Shwarz FSV	+	+	+		+	+	+		+		-	-	-	-	
Rohde&Shwarz FSW	+	+	+		+	+	+		+		-	-	-	-	
Rohde&Shwarz FSU (ESU)	+	+	+		+	+	+		+		-	-	-	-	
Rohde&Shwarz PR100 (EM100)	+	+	+		-	-	+	-	+	-	+		+	+ (low quality)	
Narda NRA6000	+	+	+		-	-	+	-	+	-	+		+	+ (low quality)	
Narda IDA 3106	+	+	+		-	-	+	-	+	-	+		+	+ (low quality)	
RS KassandraMK	+	+	+		+	+	+		+		+		+	+	
SignalHound BB60A	+	+	+		+	+	+		+		+		+	+	

AM and FM analogue signal demodulation

AM and FM analogue signals demodulation is possible for instruments that send a real-time flow of IQ data (currently available only from software defined radios or spectrum analyzers). Demodulation is possible over any frequency range provided by the instrument– from the maximum down to 200 Hz. For AM signals phase-locked loop techniques may be possible

DECT

Demodulation of DECT signals provides detection of base station addresses (RFPI addresses) and connected handsets which are in active mode (talk mode). For each base station and active handsets, signal level is determined in order search for them using amplitude direction finding techniques. Determining the list of legal addresses of a DECT base station allows the operator to discover any new DECT voice data channels present in a controlled premise, which might be used as radio microphones. RadioInspector does not perform voice demodulation as DECT uses data encryption.

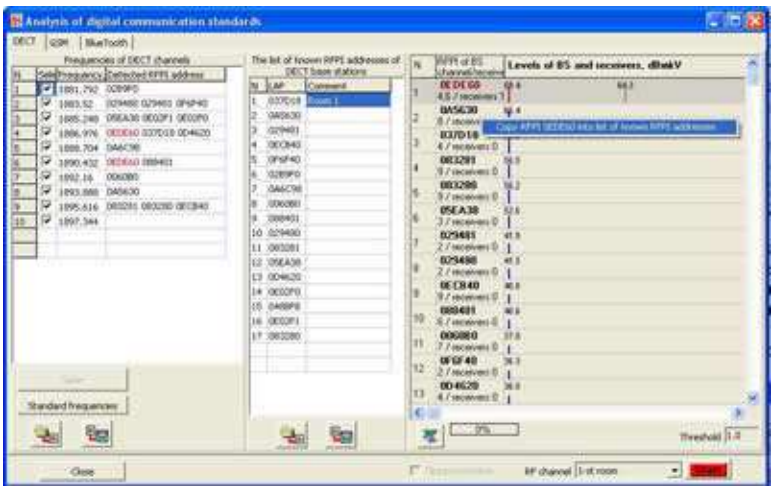

Figure 1. Signal analysis (DECT standard)

TETRA

Demodulation of a TETRA signal determines the values of MCC, MNC, ColorCode and other signal parameters. These parameters may be used for monitoring of TETRA transmitters operating properly. If the "DMO" mode is in use ("DMO" mode is a mode where 2 handsets have a direct connection with the ability to activate one handset from another) RadioInspector pops up a warning message about "DMO" mode. DMO mode can very easily be used to turn a TETRA handset into an illegal and clandestine radio frequency-based listening device for creation and activation of clandestine. Demodulation of voice is possible if encryption is not used.

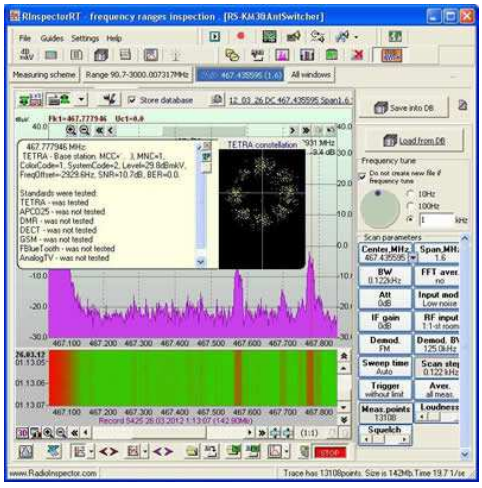

Figure 2. Signal analysis (TETRA standard)

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.

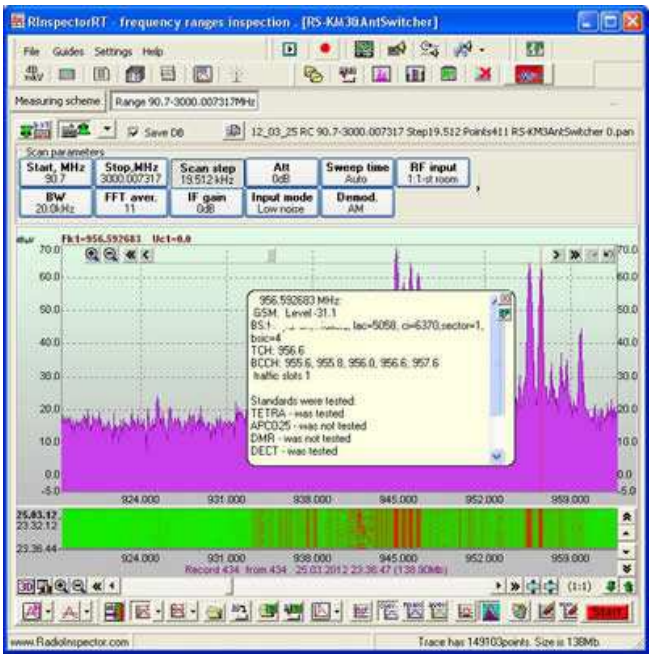

Figure 3. Signal analysis (GSM standard)

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.

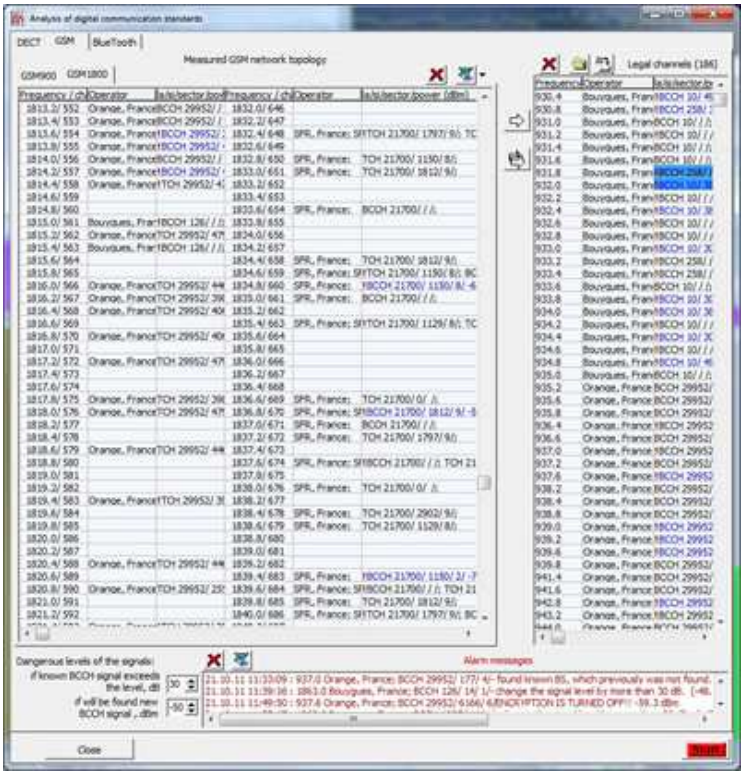

Figure 4. GSM network topology analysis

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.

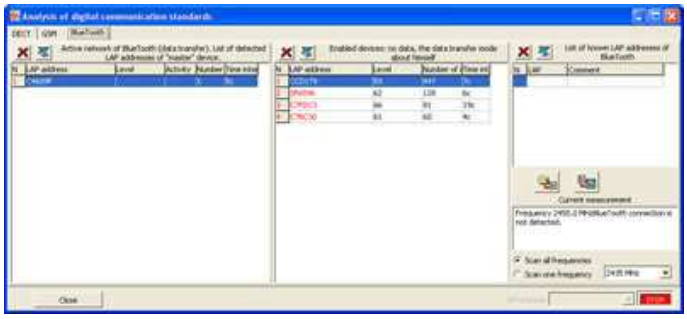

Figure 5. Signal analysis (BlueTooth standard)

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.

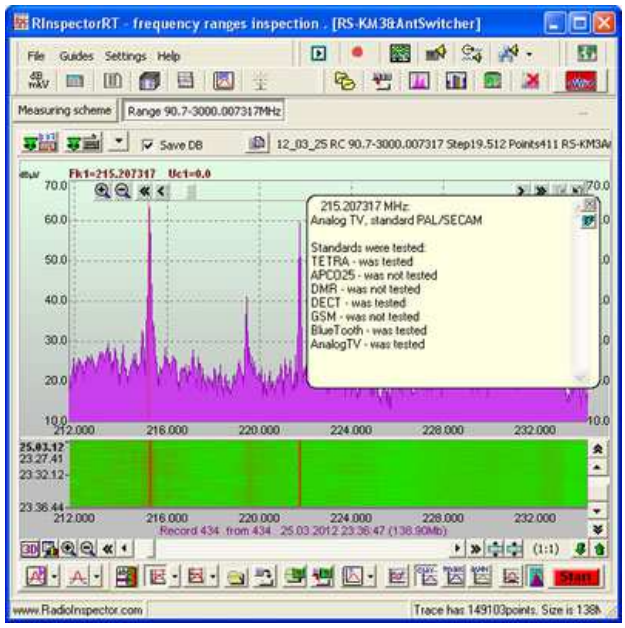

Figure 6. Radiation analysis (Analog TV)

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.

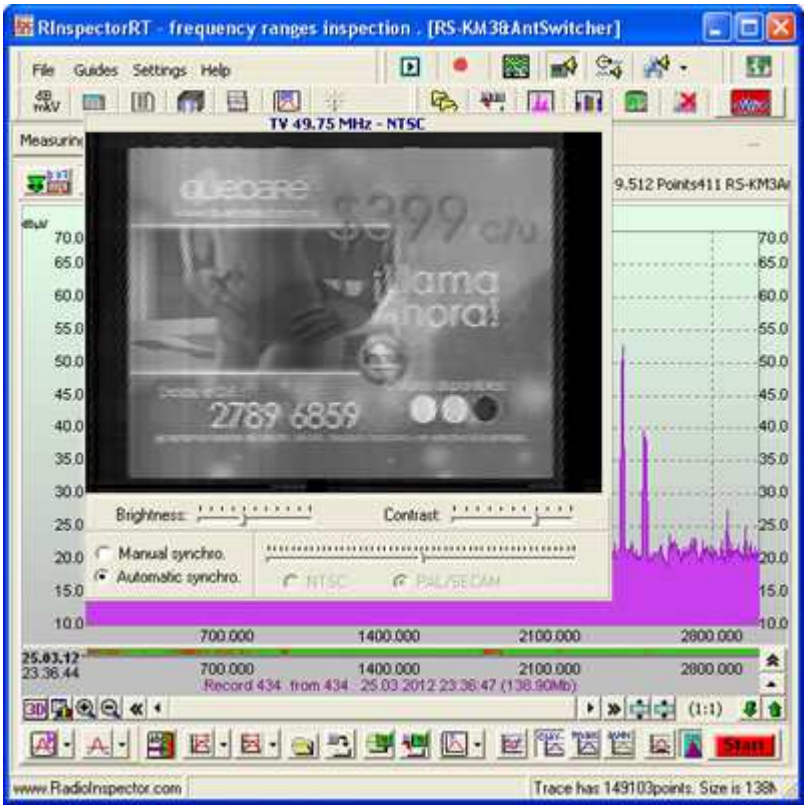

Figure 7. Video frame (Analogue TV)

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.

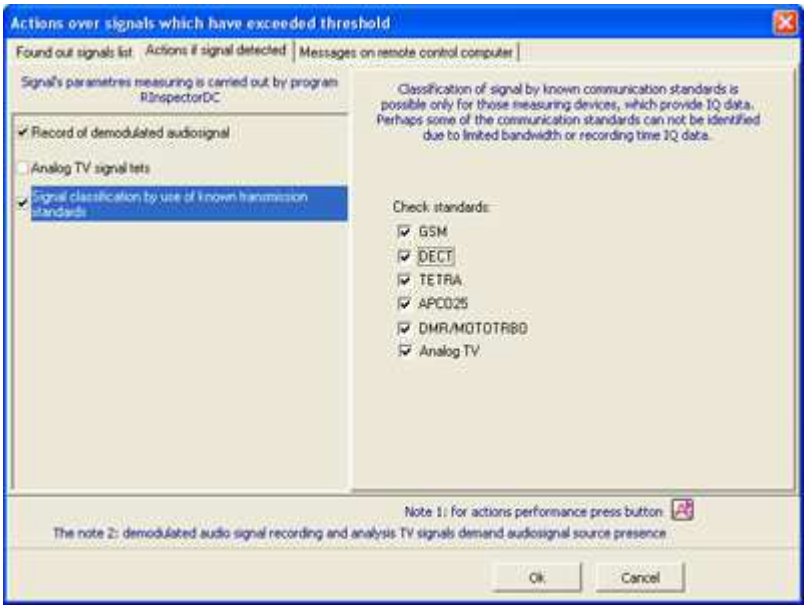

Figure 10. Software utility for signal analysis of communication standards

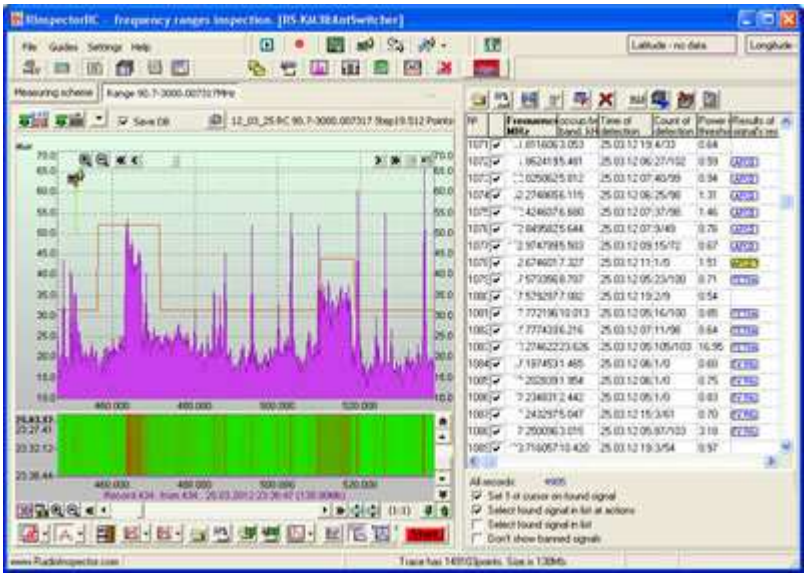

Figure 11. Results for automatic signal analysis and classification

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".