

Solutions for countersurveillance and the protection of conversations

2014



Digiscan Labs.

Securing Information Digitally

PROTECT 1207i

Multi-channel detector of wireless protocols

The Protect 1207i is a new measuring device which can be successfully used by engineers or counter surveillance specialists as a reliable tool for tracing different digital transmissions such as GSM, Bluetooth, etc. New methods of 'listening and watching' with the help of modern technologies has become widely spread in our times. For example, a tiny GSM transmitter is accessible at practically any internet spy-shop for only 100-200 USD and can listen to all your conversations in the office or at home. And perhaps more importantly the Bluetooth protocol has been specially designed to transmit voices or conversations with high quality at a distance of up to 100 m - it can easily be used for bugging.

The sensitivity of a common RF detector (bug detector) is spread along a wide frequency range, usually 3, or even 6-7 GHz. This means the common detector cannot detect such weak and non-continuous signals as Bluetooth, Wi-Fi or Wi-Max. Even more powerful signals like GSM-1800 are also hard to detect because of their low sensitivity at higher frequency ranges.

The only way to reliably detect wireless protocols is to use pre-selector chips (saw filters) which attenuate all other signals except the desired ones. This is the method implemented in the Protect 1207i which has 6 channels for different frequency ranges and can simultaneously detect 6 different kinds of transmissions at a distance much greater than any common RF detectors.

Such qualities make the Protect 1207i a very desirable and reliable device during counter surveillance sweeps.

Features

- Portable device for the inspection and location of wireless sources
- 6 channels of detection for different kinds of protocols
- Detection of GSM/CDMA/3G/DECT/LTE
- Detection of Bluetooth/Wi-Fi/Wi-Max
- Can be used for tracing both regular sources and illegal eavesdropping devices
- 6 bar graphs with 10-segments each, for accurate location of RF sources
- 4 modes: Silent, Vibration, Visual and Listen
- 2 levels of sensitivity (attenuator)
- Extra display shows probable protocol
- Durable metallic body
- Microprocessor controlled
- Setup mode with selection the threshold level for vibration.



Detect the following kinds of bugging devices:

- Bugging devices using GSM/3G/LTE standards
- Alarm systems and baby monitors with 'Listen' function
- Spy phones
- Bluetooth bugging devices
- (illegally pre-programmed)
- Wi-Fi/Wi-Max bugging devices
- GPS Trackers
- Wireless videocameras

2.4/5.8 Ghz

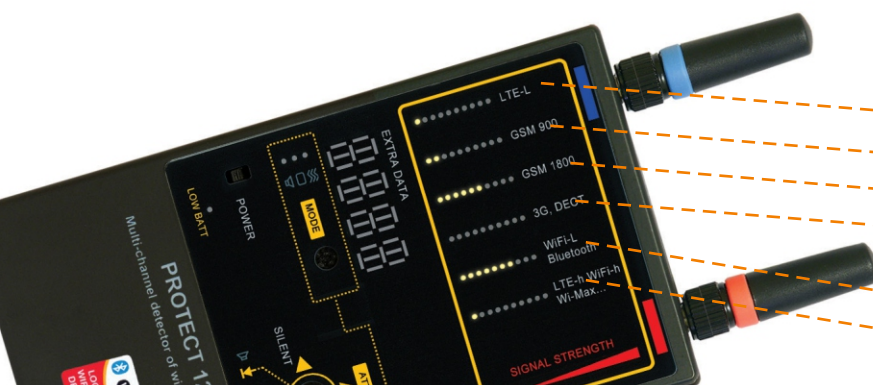
Specification

Frequency range (up-link bands)	
CDMA, LTE800 (4G)	824-849 MHz
GSM	880-920 MHz
GSM (DCS)	1710-1790 MHz
WCDMA, 3G, GSM (PCS), DECT	1920-2000 MHz
Bluetooth, Wi-Fi	2400-2480 MHz
Wi-Max/Wi-Fi High/LTE (4G)	2500-7000 MHz
Out of band attenuation	20-45 dB
Antenna	2 Omni-directional antennas
Detection distance	1-10 meters
Operation time	10-15 hours
Power	2 AAA (LR03) batteries
Dimensions (without antennas)	120 x 70 x 16 mm
Weight	217 g

Bargraphs

The Protect 1207i has 6, 10-segment, 'SIGNAL STRENGTH' bar graph indicators providing the following precise information to the operator:

- CDMA/LTE800 (4G) standard
- GSM 900 standard
- GSM 1900 and CDMA 1900 or GSM 1800
- WCDMA (UMTS, 3G), most of the modern DECT telephones or as above plus GSM 1900 and CDMA 1900
- Wi-Fi access points and adapters, Bluetooth devices
- All transmitters in the range of 2.5-7 GHz, including most kinds of the Wi-Max, Wi-Fi High/LTE (4G) protocols



Features

The perfect tool for searching for digital and analogue transmitters in the frequency range:

- Main antenna 50-6000 MHz
- Auxiliary antenna 2.4 - 2.48 GHz, 4.9 - 5.875 GHz
- Increased sensitivity to the Bluetooth/Wi-Fi signals allows operator to detect wireless sources at distance of 50 cm - 2 m
- Identification (recognition) of the type of digital transmission: GSM, Bluetooth, Wi-Fi, DECT
- 16-segment bar graph indicator providing wide dynamic range
- 4 work modes: silent, sound, vibration and mixed
- Correlation function discovers FM-transmitters by the presence of correlation (probing sound is used)
- 2 levels of sensitivity (attenuator)
- Good resource of battery (Long battery life)
- Durable metallic body
- Microprocessor controlled
- The 'CITY' antenna: for decreasing interference in an urban environment is included in the supplied set

The Protect 1206i is a new class of a counter surveillance device. Unlike all typical searching devices it can detect modern 'hidden' bugs which use such protocols as Bluetooth and Wi-Fi. Such bugs, especially Bluetooth types, are practically undetectable by common RF detectors due to their very low transmitted power and a special type of modulation. The Protect 1206i uses a separate channel with a high, (2.44GHz) frequency pre-selector to detect and locate Bluetooth and Wi-Fi with a much higher sensitivity. The unit also then processes the demodulated signal in order to identify which protocol has been detected.

In addition the unit can detect all types of 'conventional' bugging devices (FM-modulated transmitters, digital transmitters, GSM-bugs, etc.) using its distinctive features:

- Active correlation: inspecting dangerous places with the probing sound impulses while watching the 'demodulation' bar graph
- Recognition of type of digital transmission: GSM, Bluetooth, Wi-Fi, DECT
- 4 working modes: silent, sound, vibration and mixed
- Wide dynamic range thanks to the 16-segment bar graph



Specification

Frequency range	Antenna 1: 50-6000 MHz; Antenna 2: 2.4-2.48 GHz, 4.9-5.875 GHz
Power	Two AAA batteries (2xLR03)
Dimensions	Without antennas: 120x70x16 mm With antennas: 220x70x16 mm
Current consumption	Up to 30 mA
Operation duration	Up to 20 hours
Indications	Active antenna, Low battery, Mode, Identification, Attenuator, Secondary demodulation

Controls

1 ANTENNA

1. Used for the detection of the wide frequency range 50-6000MHz in order to perform searches for all types of transmitters, including room, car, body-worn, telephone or other types which use 'classical' methods of transmission, including FM modulation, GSM or other digital transmissions.

2 ANTENNA 2. Used for the detection of the Bluetooth, Wi-Fi and other transmitters working in the 2.4GHz range.

3 DEMODULATION display. Assists in an active correlation mode.

Fluctuations appearing simultaneously with the beeps will warn of an FM transmitter or other type of transmission which correlates with the sound.

4 MODE selector:

- silent mode
- sound mode, when the unit's speaker produces demodulated sound
- vibration mode, when the unit's vibrator turns on when a high level of the RF field is reached (i.e. 6th segment of the bar graph)
- mixed mode, when both types of indication are used

5 IDENTIFICATION. Changes color depending on the detected protocol: BLUE=BLUETOOTH; GREEN=Wi-Fi; RED=GSM900/1800; ORANGE=DECT

6 BARGRAPH indicator

7 POWER switch

8 ATTENUATOR function.

Used when there are many background noises in the area which can create difficulties for a search

9 Antenna selection (ANT1, ANT2)

10 CORRELATION function.

Simultaneous fluctuations on the DEMODULATION display will warn of danger

11 LOW BATT indicator. Will turn on when the batteries are nearing exhaustion.



Features

- Reliable and tested device for different sweeping tasks
- Detect both analogue and digital transmissions
- Allows the operator to locate the source
- 10-segment indicator of RF level
- Vibrating signal for concealed indication of a high RF level
- Adjustable sensitivity
- Frequency range 30MHz-6GHz
- Durable duralumin case
- Powered by 2 AAA batteries
- High sensitivity
- Last version includes the 'CITY' antenna; allowing the device to avoid interference from external sources in cities or near broadcasting towers etc.



The Protect 1203 will detect different types of radio transmitting equipment and inform you by way of a bargraph indicator or silently by a vibrating indicator. Currently there are a lot of commercially available surveillance devices that allow you to pick up different information from your office, apartment or car. These bugging devices work within different frequency ranges and have different modulation and scheme types. They may transmit using standard modulation as well as non-standard.

The Protect 1203 can detect all of these bugging devices when in active mode. You can test premises, cars or any type of items; including office equipment. You will also be able to check people for body-carried transmitters. You may perform covert sweeping using the vibrating indicator.

You will also detect if somebody is using a GSM phone. There are known cases, when people have left their mobile phone off the hook and all the conversation was transmitted to another phone or even recorded onto an

answering machine. In addition, there are plenty of GSM devices available on the market which can be used for surveillance and monitoring - GSM baby-watches, GSM-based alarm systems and different 'bugs' transmitting conversation via the mobile network.

Preparation of the Protect 1203 for sweeping is very simple. First, you switch the power on and tune the sensitivity to correct level. You then enter the room to be checked and begin to move the device in all directions and watch the indicator. You can also use the device in vibrator mode if secrecy is needed.

The housing of the Protect 1203 is made of a durable duralumin material, which protects the device from being dropped, humidity and other unfavorable conditions.

Applications (Protect 1203 / Protect 1205M)

- Searching for active radio transmitting surveillance devices (or RF bugging devices) in premises, vehicles and items.
- Room, body-carried, telephone and car bugging devices can also be found by the device.
- Discovering the improper use of mobile phones and other communication equipment for picking up conversations. The information in this case can be transmitted to another phone or recorded onto an answering machine.
- Detection of GSM bugs, 'spy' mobile phones and mobile phones in an active state (for illegal transmission of conversations)
- Detecting of harmful emissions from the GSM-jammers or mini recorder suppressors
- Detecting of harmful emissions from microwave ovens, communication antennas and other electronic appliances

Features

- Working frequency range 30-6000 MHz
- 8-segment bar graph indicator for precise measuring the radio field level and location of a bugging device
- 'Adjust sensitivity' button for omitting insignificant background fields
- Pen-style design for covert operation. Does not attract people's attention when used or transported. Can be carried in a pocket and used at the same time. Very convenient for checking surrounding objects when on a business trip, in a restaurant, hotel or somebody's office
- "High Power" indicator for pocket use
- "Pulse" indicator for recognizing digital transmitters including GSM and DECT
- Powered by LR03 battery (size AAA)

Specification	
Frequency response	30 MHz - 6 GHz
Power supply	2 x AAA / LR3 / R3
Power consumption	
with one green segment on	65 mA
with all the green segments on	80 mA
with active vibrator	145 mA
Continuous operation	Approximately 10 hours

PROTECT 1205M

Portable bug detector





Applications

- Searching for active radio transmitting surveillance devices (or RF bugging devices) in premises, vehicles and items
- Discovering the improper use of mobile phones and other communication equipment for picking up conversations. The information in this case can be transmitted to another phone or recorded onto an answering machine.
- Detection of harmful emissions from GSM-jammers or mini recorder Suppressors
- Detection of harmful emissions from microwave ovens, communication antennas and other electronic appliances

Main features of the iProtect 1210

- Detection of all kinds of active radiotransmitting devices including digital signals
- Operation driven by microcontroller
- Card-style durable body. Does not attract people's attention when used or transported.
- Working frequency range 50-3000 MHz
- 4 working modes: Normal, Sound, Vibro and Sleep
- 8-segment bar graph indicator for precise measuring of the radio field level and location of a bugging device
- Integrated antenna
- Calibrated sensitivity for rejection of background fields
- "Low battery" indicator
- "Pulse" indicator for recognizing digital transmitters including GSM and DECT
- Powered by a CR2430 lithium battery

Controls

1 'Pulse' indicator

This LED lights up when a pulse field is present near the unit. Such a field is usually produced by GSM/DECT telephones or can be created by a bugging device with a 'non-standard' type of transmission.

2 Indicators of working mode

3 Button for selection of working mode:

- **Normal.** In this mode the iProtect 1210 will indicate an increase of the RF level on the bar graph. No sound will be produced.
- **Sound.** In this mode the iProtect 1210 will produce the sound of a demodulated signal. In close vicinity of the FM-modulated bugging device a loop-back effect should appear. A buzzing sound will appear near digital transmitters like an active GSM phone. This mode allows the user to identify the transmitter.
- **Vibro.** This mode is used for covert operation or for situations when the operator cannot watch the bar graph. An increase of the RF level will cause the builtin vibrator to activate.
- **Sleep.** In this mode the iProtect 1210 'wakes up' every 3 seconds and checks the current RF environment. If there is an increased level the unit will indicate this with an alarm sound. The detector will stay active until the high level disappears.

4 This indicator turns on when the battery is low and should be replaced.

5 Power on/off

6 Speaker

7 Bar graph indicator. Displays current level of the electromagnetic field and helps the user to locate bugging devices. Location is carried out by moving the unit into the strongest level area. The bar graph consists of 8 LEDs and shows the current level with the help of 3 of them at any one time. As the field becomes stronger this group scrolls up. For powerful signals the group goes up further until two or one diode remains on.

8 Indicator of the current sensitivity level

9 Zeroing the sensitivity of the detector according to the current RF level. The unit will store the current level and clear the bar graph so that it will show stronger signals only. Perform this action before approaching the target zone or when you are trying to locate the RF source. Use this control each time it is necessary to retune the sensitivity — when you enter an area with a lower or higher level of background noise.





Features

- Was designed by TSCM/countersurveillance professionals and will protect you against all types of eavesdropping when used in correspondence with the recommendations.
- Employs a new approach to the problem of conversation protection. Uses a new, speech-like noise which, in the most of cases, has proven to be more efficient when compared to white noise.
- The noise has been 'compiled' using real human conversations and is similar to the noise of a 'rabble' in busy public places. This type of noise is the most

Usage

Please note that the MNG-300 Rabblar is just a tool, complementing and reinforcing the measures taken to protect you from eavesdropping and recording. First of all the security of your conversation depends on yourself, and later from the device. Therefore, during sensitive negotiations it is important not to increase the volume of your voice. Imagine that you are sitting in a crowded coffee shop and do not want to be heard by the people at the next table; that means your speech should not be too loud. If possible, lean forward towards your interlocutor or sit closer to each other, then place the generator on the table between you.

It is not advisable to use only one MNG-300 Rabblar if the number of participants is more than 4. In this situation, it may be necessary to use one or two additional devices. Also, while in use do not hide your generator, e.g. in your pocket or a bag! Your conversation should be "drowned" in noise; therefore the unit should be as close to the speakers as possible.

Specification

Frequency range	300 Hz - 3600 Hz
Power	9V
Current consumption	Up to 120 mA
Dimensions	85x53x21 mm
Controls	Power, Volume Indicator, Level

effective when creating interference to voice recorders and listening devices, especially when the size of the protective device is critical.

- Is a portable, cigarette-pack sized device which can easily be transported in a pocket or a small bag.
- Has been specifically designed for situations when the safety of conversations is extremely important on the one hand, and on the other hand the protective device should be as small as possible to allow easy transportation while not giving away your intentions.

As the Rabblar is always nearby, it can easily be taken out and used anytime with the slightest chance of any information leakage.

- Kinds of listening devices rendered useless by the new MNG-300 "Rabblar" Edition:

- Voice recorders
- Radio microphones
- GSM/3G "bugs"
- Body-carried video cameras - watches, ties, etc. (jamming of acoustics)
- Wired microphones
- Any other type of audio surveillance

- The MNG-300 Rabblar creates additional barrier interference which masks your speech. It is when a certain noise level is reached that listening devices will record or transmit information, it is extremely difficult, or impossible, to extract the speech component. Since the generator creates a 'speech-like' noise, the cleaning of this sound is extremely difficult or most likely impossible, if the level of noise is sufficient.

- The housing of the unit is made from a very reliable material and is extremely durable, guaranteeing a long life for the device.

- The size of the MNG-300 Rabblar is comparable to a pack of cigarettes and can even be carried inside one in order not to attract attention, although an attractive leather case is supplied.



Protection of conversations against all kinds of eavesdropping



Top-of-the-line protection system. This is the only device in the world which can give 100% protection to your conversations against interception or recording. The DRUID D-06 creates powerful interference against all kinds of listening devices! Even if a person is standing next to the participants, they will not be able to understand what is being said. The headsets allow the users to hear each other clearly while the DRUID's central unit produces interference. Powered from 220V or the internal rechargeable battery with a resource time of 4-6 hours. The unit is supplied in a carry case.

Not all listening devices can be detected by existing methods. The DRUID D-06 is a unique system for providing protection of human's speech.

Remotely controlled radio microphones, wired microphones, passive resonators, miniature voice recorders practically all these devices cannot be detected by conventional methods. Even a modern cellular phone may contain a digital voice recorder; this means that any phone lying on the desktop could be used by an adversary to record a conversation.

Therefore it is extremely important to have a reliable device protecting private conversations, not depending on their level of importance. The concept of the DRUID is based on generating audio interference produced simultaneously with a human's speech. The volume of this interference is higher than a person's voice; therefore neither listening device nor recorder is able to pick it up.

The generated audio interference cannot be cleared by any noise-clearance methods. At the same time the produced interference does not create any inconvenience to the participants of the negotiation thanks to the special headsets. The DRUID headset allows users to hear each other with crystal clear quality.



Headset for DRUID D-06

Features

- Professional system for protecting speech between up to 6 persons
- Protects against all known methods of listening, including all types of radio microphones, stethoscopes, voice recorders, passive resonators, wired microphones, etc.
- The system uses usual multimedia headsets. 4 headsets PLANTRONICS AUDIO 355 included in the standard set
- Absolutely harmless to your health: no microwave reflections or ultrahigh sound noise
- Compared to a white-noise generator the DRUID provides a much higher level of protection;
- The system is portable: supplied in a plastic carry-case it can be easily prepared for use;
- Powered from an internal rechargeable battery the DRUID D-06 can work for up to 6 hours without mains supply;
- The system can be used in any situation, it is especially valuable when conducting highly important negotiations in an unknown environment



Supplied set

Specification

Type of noise	Distortion+Reverberation
Number of channels	6
Power source	AC 220V / rechargeable battery
Duration of work from internal battery	4-6 hours
Dimensions	23x6.5x17 cm

DNG-2300 protects from:

- Laser and microwave surveillance systems using reflections from windows
- Electronic stethoscopes (contact microphones)
- Microphones built in the walls or other constructions
- Other vibro-acoustic methods of information leakage

The DNG-2300 generator has been created to protect against listening devices which cannot be discovered by common methods. The unit protects a room by inducing non-filterable noise onto surfaces. This noise, also known as 'white' noise, is transmitted onto surfaces with the help of the TRN-2000 transducers and OMS-2000 speakers in the unit. The number of transducers and speakers is dependent on the room's configuration.

Thanks to the TRN-2000's transducers the protection level of the generator is higher than systems which only have speakers. The transducers pass most of the generated noise into the desired construction in the form of vibration while producing less audible interference. Although a slight noise may be heard inside the protected area there will be no need to raise your voice.

How the eavesdropping works

Vibration-acoustic leakage is possible thanks to the ability of sound waves to penetrate walls, windows and other constructions. In some materials sound travels even better than in air. For example, water is a great conductor of sound and a heating system can be easily used for picking-up peoples' speech. This principal is used in electronic stethoscopes. They pick up vibrations caused by conversations on walls, windows and other constructions and transform them back into sound. These eavesdropping devices can be installed, not only in the adjacent premises, but even over a number of floors or rooms which are somehow connected to the target area - by mutual cavity or construction.



Principal of protection

The DNG-2300 can 'block' the above methods. This is carried out with the help of special transducers. It is recommended to use the REI's TRN-2000. Their parameters are optimal for many kinds of surfaces. The TRN-2000 are very efficient which means that only an insignificant part of the produced noise will be let into the air, while most of it will be 'injected' into the construction in the form of vibration. With the help of the bracket the transducers can be mounted onto practically all kinds of surfaces.

The OMS-2000 omni-masking speakers can also be used with the DNG-2300. Their purpose is to produce non-filterable noise in spaces like ventilation shafts, behind ceiling tiles, etc.

Transducers and accessories for DNG-2300

TRN-2000 Transducer



Designed for the protection of walls, windows, ceilings, floors and pipes. One transducer protects a section of about 3x3 meters of a wall, one Window pane or a pipe of water supply or heating system. Quantity in other cases may vary.

OMS-2000 Omni-masking speaker



Designed to produce non-filterable noise in spaces like ventilation shafts, behind ceiling tiles, etc. Can also be used to create interference for voice recorders and other bugging devices within the room.

Specification

Digital noise generator DNG-2300	
Dimensions	6.0 x 17.5 x 25.4 cm
Weight	2.2 kg
Transducer channels	
Max. output power	2 x 10 W
Frequency response	250-5000 Hz
Min. impedance of load	3 Ohm
Acoustic channel	
Max. output power	1 x 8 W
Min. impedance of load	8 Ohm
Frequency response	250-6500 Hz
Power	220V 50 Hz
Transducer TRN-2000	
Dimensions	37.6 x 3.1 cm
Weight	454 g
Impedance	6 Ohm
Omni-masking speaker OMS-2000	
Dimensions	12.7 x 14.6 cm
Weight	907 g
Impedance	24 Ohm
Test microphone DNG-MIC	
Output level	1 V
Weight	110 g

Detector of the illegal activation of mobile phones



The GSM-BOX 2 has been designed to detect and indicate the illegal activation of a mobile phone. In addition to this main function, the GSM-BOX 2 also creates interference to the surrounding area of the telephone's microphone by generating 'white noise' when radio-waves are detected; this noise suppresses the microphone in the telephone rendering it useless.

Features

- Warns you with the help of the 3 LEDs and a sound alarm when the telephone starts exchanging data with the network
- Automatic generation of audio interference
- Accurate and sensitive detection of GSM 900/1800, CDMA850, WCDMA2100 (3G, UMTS) and Wi-Fi/Bluetooth by an intelligent algorithm of the microcontroller
- Separate visual and sound indication of different communication protocols
- New convenient 'credit card-style' design suitable for pocket use, belt carrying cases, bags, desktop stands, etc.
- A new sensitive scheme of detection with pre-selectors provides a better detection distance
- Long battery resource of up to 5 days (low current consumption)
- Does not block the mobile network in the area
- Has no adverse effect on health (no electromagnetic waves)

Specification

Detected protocols	GSM 900/1800, CDMA850, WCDMA2100 (3G, UMTS) and Wi-Fi/Bluetooth
Frequency range of generated interference	300-5000 Hz (white noise)
Sound pressure level in the area of the speaker	90 dB
Power source	3V, CR2430 battery
Current consumption	3 mcA/15mA standby/noise)
Dimensions	100x50x5 mm

GSM-SAFE 3

Detector of the illegal activation of mobile phones with protection function



Modern communications give varied possibilities of information exchange. At the same time these devices can become a dangerous tool for picking up information illegally. A reprogramming of your mobile phone, installing spyware in it, the substitution of it, or being given a modified telephone will all give other people access to the data in your handset, or the ability to listen to all conversations around you from anywhere in the world. Such illegal actions can be accomplished without any signs on the display being shown or sound signals being heard.

The GSM-SAFE 3 has been designed to detect the illegal activation of a mobile phone. In addition to this main function, the GSM-SAFE 3 also creates interference to the surrounding area of the telephone's microphone by generating 'white noise' when radio-waves are detected; this noise suppresses the microphone in the telephone rendering it useless.

Features

- 2 working modes:
 - 1) DETECT - warns you with the help of the LED when the telephone starts an exchange of information;
 - 2) NOISE - in addition to warning the GSM SAFE 3 will produce audio interference which suppresses the telephone's microphone
- Accurate and sensitive detection of GSM 900/1800, CDMA850, WCDMA2100 (3G, UMTS) and Bluetooth/Wi-Fi by an intelligent algorithm of the microcontroller
- This latest version turns on automatically when a telephone is put inside and automatically turns off when the handset is taken out.
- Indication of detected communication protocol by the color of the LED
- Produced as an attractive wooden desktop stand
- A new more sensitive scheme of detection with pre-selectors provides a better detection distance
- Long battery life of up to 10-15 days when used moderately
- Does not block the mobile network in the area
- Has no adverse effect on health (no electromagnetic waves)
- Compatible with virtually all types of GSM telephones (max width 7 cm, practically any height and thickness)

Specification

Detected communications	GSM 900/1800, CDMA 850, WCDMA 2100 (3G, UMTS) and Wi-Fi/Bluetooth
Frequency range of acoustic noise	300-5000 Hz ("white noise")
Power	3V, 2 x AAA
Current consumption	1,2 mA/50 mA (stand-by/active)
Detected	102x84x74 mm

Features

- Detection of all types of hidden video cameras not depending on their working state
- Distance of detection between 2 and 10 meters
- IR filter for rejection of natural reflections
- Adjustable power of radiation
- Powered by 2 AAA batteries
- Battery discharge indicator
- Size 140x34x16 mm

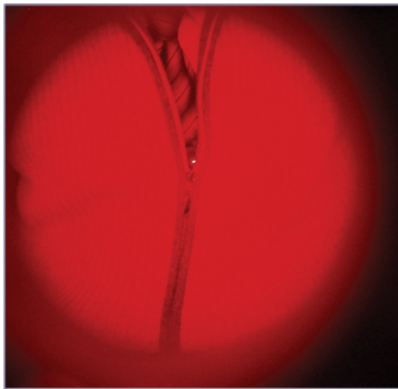
This unique device was created for professionals in the sphere of the surveillance countermeasures. Thanks to its optical principle the "WEGA i" can discover lenses of all types of covert cameras not depending on their working state.

The WEGA's LED matrix radiates a powerful infrared beam which is then reflected by a video camera's optics and is easily detected by the operator.

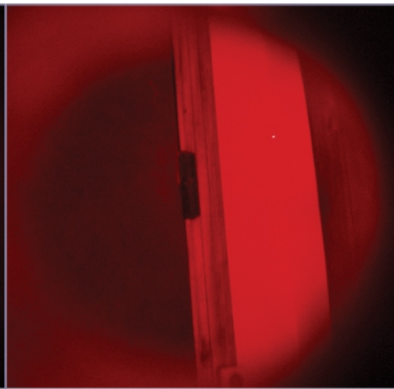
The IR-filtering glass built into the “WEGA i” helps the operator to avoid natural reflections from surfaces and concentrate on finding the exact location of a hidden camera.



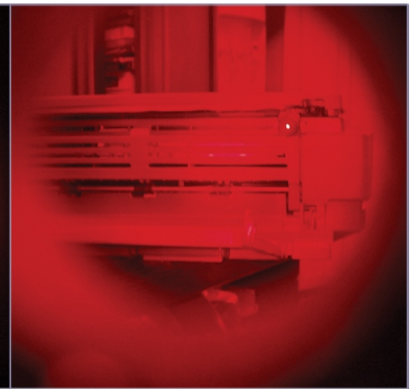
Examples of detection



Body-carried video camera in a tie



Video camera in a wall



Video camera in a copying machine

Examples of video cameras which can be found by WEGA i:





Features

- Quickly and reliably detects eavesdropping devices which use the RF waves, wires and infrared beams for transmission of information from the premises
- Types of detected bugs: VHF / UHF radio microphones, GSM/3G bugs (GSM baby), digitally encrypted radio microphones, telephone transmitters, AC/telephone line/Ethernet carrier transmitters, hidden video cameras with transmitters, microphones with transmission via the infrared beams, hidden electronic devices in objects
- 2-antenna analysis provides quick selection of the RF signals originating from the checked rooms not depending on the modulation type
- Measurement are accomplished with the help of the modern digital receiver, providing spectrum analyzing possibilities with the scan rate of 50 MHz per second at 12.5 kHz resolution
- Detects intermittent (non-constant) signals with the help of the Sonogram function
- Wide frequency range covered: 5 kHz – 4400 MHz (ver. 4G) and 5 kHz -12400 MHz (ver. 12G)
- Built-in low-frequency convertor provides features for inspection of the wires, electro-magnetic range and the infra-red range
- Working modes: RF sweep, Microwave check, AC check, TLF check (telephone/low-voltage wire), IR check (infrared optical range), MLP check (electromagnetic probe), Detector-Locate
- Detector-Locate mode allows the operator to find the physical location of the transmitter
- Digital communication sources (GSM, Wi-Fi, Bluetooth, 3G, LTE, Wi-Max, etc.) can be inspected and located
- Automatic data logging provides possibility to accumulate signal's history during the searches
- Wide set of graphical elements: Spectrum (current, max, min, remote antenna, threshold, etc.); Sonogram; IQ constellation; Oscilloscope; FFT-spectrum;
- FM/AM demodulation with selectable bandwidth
- Analysis of the modulation in the IQ constellation window
- Database stored in Microsoft Access format
- Recording of demodulated audio
- High quality RF antennas and VLF-probes included in the supplied set: 2 omnidirectional ODA-4 antennas; 1 microwave MWA-6 antenna; 1 microwave MWA-12 antenna (for version "12G" only); 1 infrared IR-LINE probe; 1 electromagnetic MLP-LINE probe; 1 110/220V probe AC-LINE; 1 telephone line/low voltage probe.

Technology

The spectrum analyzing technology used in the Delta provides the professional level of sweeping, giving full information about the radio frequencies being used in the area to the operator practically without necessity to move the equipment within the territory. The digital receiver used in the Delta has much longer distance of detection in comparison to the conventional RF detectors, so the sweeping procedure can be performed quickly and covertly, room by room. The system can be placed both inside the room being checked and in an adjacent premise to provide secrecy of operation.

The 2-antenna analysis used in the Delta allows you to detect RF bugging devices not depending on the type of modulation and encryption. Its working principal is based on the nature of radio waves to decrease power proportionally to the distance to the source. Signal on the close antenna will be stronger than the one received in the remote antenna. Such the DigiScan EX Delta system quickly selects the transmissions which originate from the inside of the premise. The system has a built-in high-quality antenna switcher.

After the sweeping the operator can perform the location procedure and find the exact location of the bug.

In addition to the RF analysis the Delta has the possibility to check the wire communications, infrared range and electro-magnetic range for presence of illegal signals. For this aim the system includes a low-frequency converter.

The Delta system and its software DigiScan EX have a simple intuitive interface and do not demand special knowledge from the operator. Typically the operation is performed in 3 stages: 1) placement of the antennas or probes; 2) pressing the corresponding operation button; 3) watching the results. At the same time professionals will find many high-grade possibilities and settings, which can be useful for deeper learning of RF environment at a further usage.

Specifications

General

- RF frequency range: 4G: 50 kHz – 4400 MHz
12G: 50 kHz -12400 MHz
- Scan rate: 4G: 75 MHz per second
12G: 50 MHz per second
- Resolution: 12.5 kHz
- Displayed dynamic range: -90 dBm to -10 dBm
- Demodulation: FM/AM
- Demodulation bandwidth: 240/120/60/30/15 kHz
- Audio bandwidth (VBW): adjustable 22kHz – 1 kHz
- Attenuator: PRE-AMP, 0dB, 5dB, 10dB and 15dB
- Inputs: 3 antenna inputs; 4 probe inputs
- Software: DigiScan EX, version 3.0 or newer
- Selectable span (manual mode): 50 MHz, 25 MHz, 10 MHz, 5MHz and 2 Mhz
- Detection of pulse transmissions: yes, pulse mode on
- Observe mode: frequency domain (spectrum); time domain (demodulation)
- Graphic windows: spectrum of wide range (selectable span between 1.5 to 3000 MHz), signal's spectrum, IQ constellation, oscilloscope, FFT-spectrum
- Real-time I/Q data streaming: at 240 kHz bandwidth
- Compatibility: Windows XP, Windows Vista, Windows 7, Windows 8
- Power source: 220 (110) V

ODA-4 omnidirectional antenna

- Can be used with any RF equipment, including receivers, spectrum analyzers, RF detectors, etc.
- Frequency range 80-4000 MHz
- Tripod mountable (tripod supplied)
- The tripod can convert to a hand-held unit for manual probing (locating procedure)
- Connector type: BNC
- 80 cm cable
- Dimensions (without tripod) 20 x 3.5 x 0.6 cm
- Mode of use: receive
- Indoor use only

MWA-6 microwave antenna

- Can be used with any RF equipment, including receivers, spectrum analyzers, RF detectors, etc.
- Is particularly good for the location of GSM, CDMA, 3G, 4G (LTE, Wi-Max), Wi-Fi 2.4GHz, Bluetooth, Wi-Fi 5GHz, DECT and other digital transmissions
- Perfectly suited for Delta 4G/12G, Protect 1206i, Protect 1207i
- Frequency range 800-6500 MHz
- Directed (log-periodic)
- Typical forward gain: 6 dBi
- Tripod mountable (tripod supplied)
- The tripod can convert to a hand-held unit for manual probing (locating procedure)
- Connector type: SMA
- 80 cm cable
- Dimensions (without tripod) 18 x 14.5 x 0.7 cm
- Mode of use: receive
- Indoor use only

MWA-12 microwave antenna

- Can be used with any RF equipment, including receivers, spectrum analyzers, RF detectors, etc.
- Is particularly good for locating digital transmissions above 2GHz: 4G (LTE on the upper ranges, Wi-Max), Wi-Fi 2.4GHz, Bluetooth, Wi-Fi 5GHz; For tracing other microwave sources, including bugging devices
- Perfectly suited for the Delta 12G, Protect 1206i, Protect 1207i
- Frequency range 2000-12000 MHz
- Directed (log-periodic)
- Typical forward gain: 8 dBi
- Tripod mountable (tripod supplied)
- The tripod can convert to a hand-held unit for manual probing (locating procedure)
- Connector type: SMA
- 80 cm cable
- Dimensions (without tripod) 8 x 6 x 0.7 cm
- Mode of use: receive
- Indoor use only

IR-LINE infrared probe

- Used in Delta 4G/12G systems for the tracing of illegal infra-red beams (IR bugs)
- Frequency range 50 kHz – 4 MHz
- Directed (angle 15°)
- IR filter rejects optical range
- Tripod mountable (tripod supplied)
- The tripod can convert to a hand-held unit for manual probing (locating procedure)
- Connector type: MiniDIN8
- 120 cm cable
- Dimensions (without tripod) 9.5 x 6.2 x 3 cm

MLP-LINE electromagnetic probe

- Used in Delta 4G/12G systems. Detects electronics emitting an electromagnetic field
- Frequency range 50 kHz – 4 MHz
- Omni-directed 360°
- Tripod mountable (tripod supplied)
- The tripod can convert to a hand-held unit for manual probing (locating procedure)
- Connector type: MiniDIN8
- Dimensions (without tripod) 18 x 6.2 x 3 cm

AC-LINE – probe for 110/220V wires

- Used in Delta 4G/12G systems for the detection of illegal signals in 110V/220V wires
- Frequency range 50 kHz – 12 MHz
- Compatible with 110V and 220V
- Connector type: MiniDIN8
- 120 cm cable
- Dimensions 8 x 7 x 3 cm

Telephone/low voltage probe

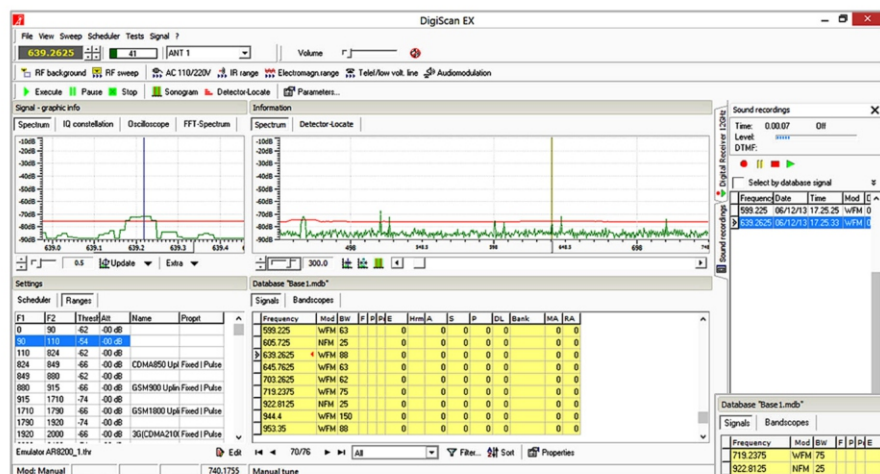
- Used in Delta 4G/12G systems for the detection of illegal signals in telephone and other low-voltage wires
- Frequency range 50 kHz – 12 MHz
- Maximum voltage 100V
- Connectors:
 - 1) modular telephone plug 6P6C;
 - 2) 'alligator' connector
- Extendable cable up to 6 meters
- Telephone splitter supplied

Supplied set

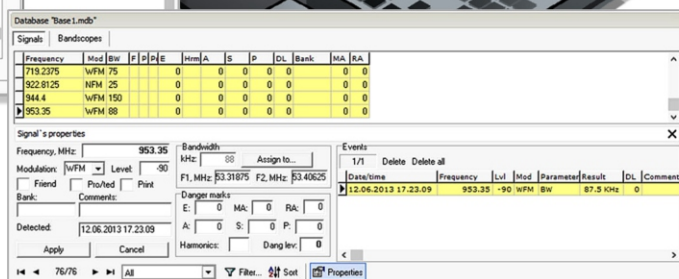


No	Item	4G	12G
1	DigiScan EX software on USB-flash drive	1	1
2	Digital Receiver SignalHound 4.4 GHz or 12.4GHz	1	1
3	USB-cable for the digital receiver	1	1
4	Controller DSC-003	1	1
5	USB-cable for the DSC-003	1	1
6	AC power adapter for DSC-003	1	1
7	DS-Line 2 Pro, VLF-converter	1	1
8	Interconnection cable "DS-Line 2 Pro – DSC-003"	1	1
9	BNC-BNC cable	1	1
10	BNC-SMA cable	1	1
11	ODA-4 omnidirectional antenna	2	2
12	High quality RF extension cable for ODA-4 antenna (20 meters)	2	2
13	MWA-6 microwave antenna	1	1
14	MWA-12 microwave antenna	-	1
15	AC-LINE, probe for AC wires	1	1
16	IR-LINE, infrared probe	1	1
17	MLP-LINE, electromagnetic probe	1	1
18	Telephone/Low voltage probe	1	1
19	Extension cable for probes, 10 m	1	1
	Cable DS-L-AR8200 for AR8200	On request	
	Cable DS-L-SND for IC-R1500/2500		

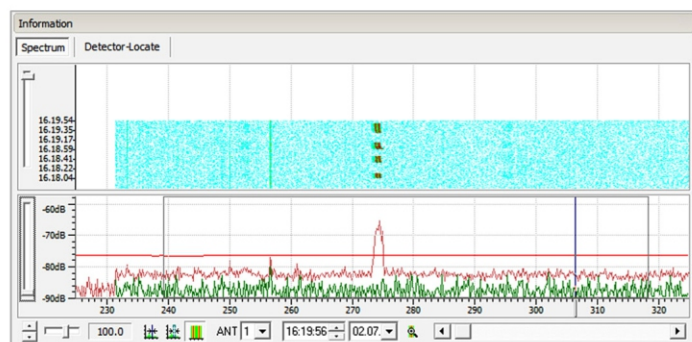
Screenshots



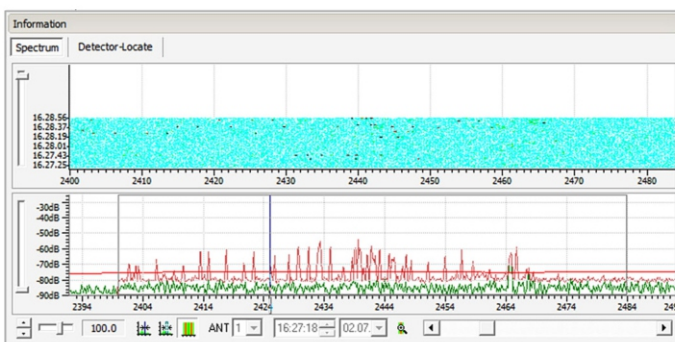
Main window



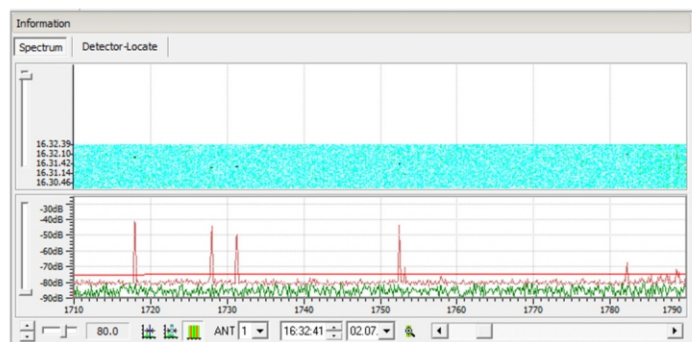
Database



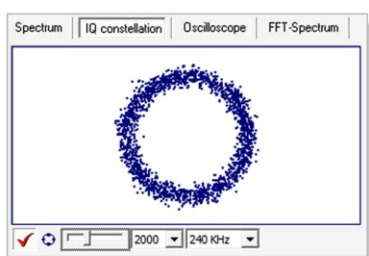
Intermittent signal detected at 274 MHz



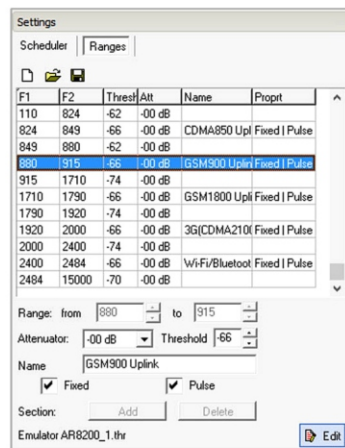
Detected Wi-Fi signals



GSM signal



IQ Constellation for FM signal



Settings - Ranges



Digiscan Labs.

Securing Information Digitally

Dealer locations:

Belgium • China • Czech Republic • India • Italy
Japan • Korea • Latvia • Lithuania • Netherlands
Pakistan • Poland • Romania • Russia
Slovak Republic • Spain • Ukraine
United Kingdom • USA

Visit our website for details:

www.digiscan-labs.com

