

Solutions for countersurveillance and the protection of conversations




Global TSCM Group
New York

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.



Detect the following kinds of bugging devices:

- GSM baby-monitors/
- GPS Trackers
- GSM alarm/GSM bugs
- Bluetooth bugging devices
- GSM/GPRS/EDGE/
- Spy phones with Bluetooth/Wi-Fi
- 3G video cameras
- Wi-Fi/Wi-Max bugging devices
- GSM Spy phones
- Wireless videocameras 2.4 Ghz

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
- 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.

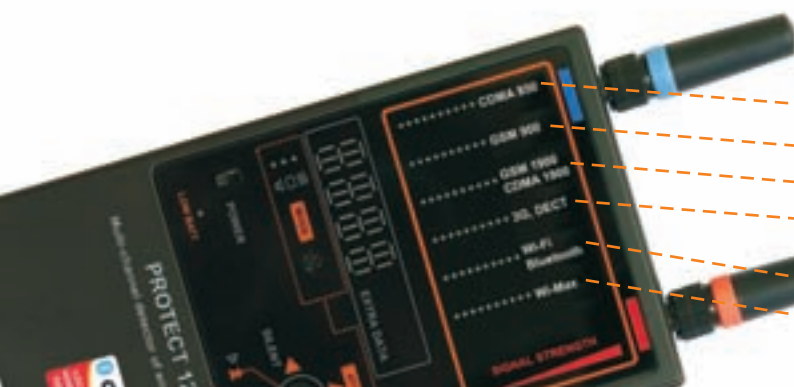
Specification

Frequency range (up-link bands)	
CDMA	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	3000-7000 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 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 3-7 Ghz, including most kinds of the Wi-Max protocol



PROTECT 1206i

Detector of bugs and digital transmissions

Features

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

- Main antenna 50-4000 MHz
- Auxiliary antenna 2.44 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
- Latest version includes the extra antenna allowing the device to avoid interference from external sources in cities or near broadcasting towers etc.

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: 50-4000 MHz; Antenna 2: 2.44GHz
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 50-4000MHz 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.



PROTECT 1203

Portable bug detector

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 10-3600MHz
- 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. In such cases you can carry the Protect 1203 about your person and stand in close proximity to a potential threat. If the vibration starts near a certain place, this indicates that the radio field is higher and there is a RF device.

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

- 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

Specification

Frequency response	10 - 3600 MHz
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

Features

- Working frequency range 50-2400 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)



PROTECT 1210

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 Protect 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 Protect 1210 will indicate an increase of the RF level on the bar graph. No sound will be produced.
- Sound In this mode the Protect 1210 will produce the sound of a demodulated signal. In close vicinity of the FM-modulated bugging device a loopback 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 built-in vibrator to activate.
- Sleep In this mode the Protect 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.



MNG 300 Skeller

Noise generator

Features

The MNG-300 Skeller will allow you to improve the security of your negotiations and protect you against listening and recording devices. When used in the correct manner the MNG-300 Skeller will protect you from:

- voice recorders (tape and digital)
- microphones, wireless microphones
- stethoscopes, laser window stethoscopes
- GSM-transmitters, etc.

The MNG-300 Skeller creates an 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 from this noise. Since the generator creates a "white" noise, which is distributed throughout the speech range of the spectrum of human voice, cleaning of the noise is not possible, 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 Skeller 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.

Usage

MNG-300 Skeller is a tool, which complements and reinforces the measures taken to protect you from eavesdropping and recording. First of all the security of your conversation depends on yourself, and then 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. Please note: it is not possible to use only one MNG-300 Skeller if the number of participants is more than 4. In this situation, it may be necessary to use additional devices from the Skeller + series.

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. Do not decrease the volume of the MNG-300 Skeller; always use it at maximum volume and speak quietly.

If your companion has a recorder about his person, he will record himself, but not you, as long as your voice is not 'over' loud.

Modern digital recorders use a compression of sound during the recording process. Such a procedure "shrinks" unnecessary pauses and removes irrelevant sounds. Thanks to this noise cleaning procedure during the process of recording digital voice recorders are more resistant to noise generators. Therefore, the recorder must "hear" more noise than speech, and therefore you must comply with the low volume of conversation and keep the generator closer to the potential location of a "bug".

Analog transmitters (radio microphones) use a classical scheme of sound processing, which clogs the noise much easier than that of digital voice recorders. I.e. wireless microphones are suppressed easier than recorders.

The MNG-300 Skeller is powered by a 9V battery and can work from 5 to 10 hours. Replace the battery by turning the screw on the underside of the housing. Turn the screw and shake the unit slightly to open the battery compartment.

If the recorder can be in an undisclosed location, somewhere around you, you may need to use an additional generator. Place 2 generators between the interlocutors, placing them in different directions, or one between the interlocutors, and the second - somewhere behind you or to one side.

Specification

Frequency range	300 Hz - 4600 Hz
Power	9V
Current consumption	Up to 120 mA
Dimensions	85x53x21 mm
Controls	Power, Volume
Indicators	Power, Level

MNG 300e Skeller+

Noise generator

Features

The MNG-300e Skeller+ will allow you to improve the security of your negotiations and protect you against listening and recording devices. When used in the correct manner the MNG-300e Skeller+ will protect you from:

- voice recorders (tape and digital)
- microphones, wireless microphones
- stethoscopes, laser window stethoscopes
- GSM-transmitters, etc.

The MNG-300e Skeller+ creates an 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 from this noise. Since the generator creates a "white" noise, which is distributed throughout the speech range spectrum of the human voice, cleaning of the noise is not possible, 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-300e Skeller+ 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.



Way of use

- The volume of the MNG-300e Skeller+ is constant, but the noise is only generated when speech is detected.
- To operate successfully it is necessary to meet certain requirements connected with the surrounding noise in the room, the loudness of a conversation and the number of units applied.
- The bar graph shows the background noise at the moment when the unit is turned on. If the red segments blink after turning it on, the surrounding noise is excessive and the MNG-300e cannot function properly. In this case it is necessary to close windows, turn off sources of noise (TV, CD-players, etc.), press the RESET button and try again.
- The audibility of speech should be sufficient to activate the unit but not be excessive.
- It is recommended to use one MNG-300e for two persons only. If there are more participants it is necessary to use one unit for each person. The MNG-300e should be placed near each person, for example, on the desktop, and then activated. If there are any other suspicious places in the room (where you know or suspect a bugging device could be) it is advisable to place a unit near each of these areas.
- The acoustic properties of premises have a serious impact on the situation, but usually, up to 4 MNG-300e can work simultaneously in a normal way.
- The MNG-300e Skeller+ is powered by a 9V alkaline battery providing a working time of up to 8 hours.

Specification

Principal of work	White noise
Frequency response	250-4600 Hz
Dimensions	2.7 x 5.5 x 8.6 cm
Controls	Power on/off, RESET
Indicators	Bar graph (10 segments)
Supplied set	Unit, leather case, battery, user manual

DRUID-D06

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 2-4 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. Each headset has a built-in RF detector which guarantees protection against bugs which can be carried in the ear.



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-600 (s)
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-600
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-600(S)	
Dimensions	60 x 24 mm
Weight	45g (600) 50g(600S)
Sound and Vibration capability	TRN-600S only
Omni-masking speaker OMS-600	
Dimensions	12.7 x 14.6 cm
Weight	907 g
Impedance	24 Ohm
Test microphone DNG-MIC	
Output level	1 V
Weight	110 g

GSM-BOX II

Detector of the illegal activation of mobile phones



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 mA/15mA standby/noise)
Dimensions	100x50x5 mm

Features

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.

GSM-BOX 2 is an updated version of its predecessor (GSM-BOX), and has the following distinctive 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)

GSM-SAFE II

Detector of the illegal activation of mobile phones with protection function



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, 2V x AA
Current consumption	1,2 mA/50 mA (stand-by/active)
Detected	102x84x74 mm

Features

- Instant automatic protection against 'spy' phones thanks to the built-in RF detector and noise generator
- Completely harmless to your health (no electromagnetic waves)
- Compatible with the GSM 900 / GSM 1800 (PCN) / GSM 1900 (PCS) / CDMA 850 / 3G
- Compatible with virtually all types of GSM telephones
- Built-in diode for active mode indication

The GSM SAFE 2 has been created to protect your conversations in case your mobile phone has been modified or changed. It has been designed to act as an attractive desktop stand. Its features include a built-in radio-frequency detector, a controlling scheme and a noise generator which activates when the phone is active. Therefore, the phone should be kept in the GSM SAFE 2 to provide 24 hour indoor protection.

Normal calls can be answered in the usual way since you will hear the telephone's melody or vibration and simply remove it from the stand. Hidden 'spy' activations do not produce any sound or vibration and this is where the GSM SAFE 2 will protect you. In the event of a 'spy' activation the GSM SAFE 2 will automatically turn on its noise generator and the listener will hear this sound only. You will also instantly notice your phone's activation thanks to the built-in LED indicator and the low sound coming from it.

- 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

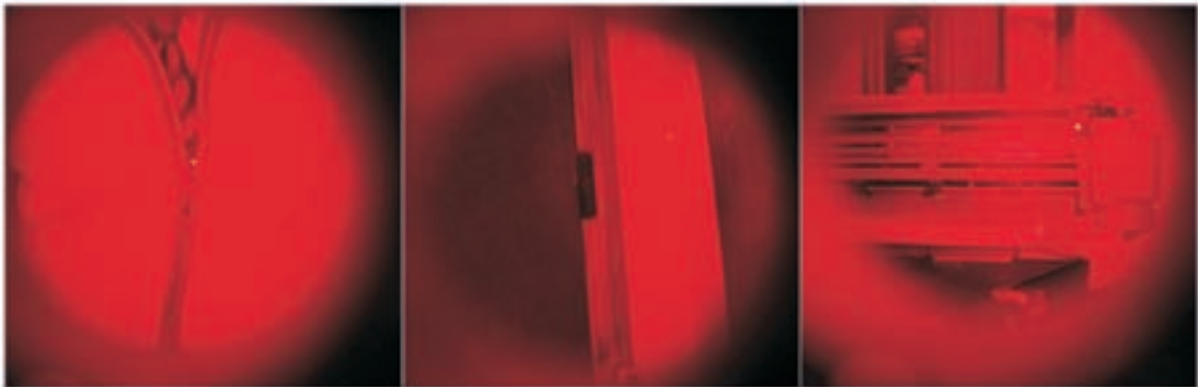
This unique device was created for professionals in the sphere of the surveillance countermeasures. Thanks to its optical principle the "WEGA i" can discover lenses of all types of covert cameras not depending on their working state.

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:



DigiScan EX

Countersurveillance sweeping system

DigiScan EX reveals all the possibilities of your receiver and allows you to perform sweeping procedures at a professional level



External view of the DigiScan EX sweeping system

Features

- Uses the standard ICOM or AOR receiver (IC-R1500/2500 or AR8200 are recommended)
- Scans RF range 0.1-3300 MHz and VLF range 5kHz -12MHz
- The software includes a wide set of algorithms for searching and signal processing
- New controller DSC-003 provides transfer of sound from receiver and built-in microphone via USB to the computer
- General and precise scanning is performed during a search; this provides an accurate measurement of the signal's central frequency
- The algorithm of the spectrum analysis qualitatively recognizes signals from the received data
- Multi-sector threshold, reference bandscope
- The Microsoft Access database format provides great possibilities for processing the results of search - filtering out, sorting, operating the clipboard, generation of reports for printing or the creation of PDF files
- Automatic sound recording can be accomplished for the detected signals
- The general radio monitoring functions allow the user to scan with a random step and mode, program the resumption conditions and carry out sound recording
- Reliability of the system is confirmed by years of effective operation on the territory of Ukraine, Russia and many foreign users
- A new algorithm 'energetic correlation' has been implemented in the new version DigiScan EX S-Pro. This method compares levels of a signal on the internal and the or combination of the threshold and bandscope can be used
- The 'Background pickup' mode allows the operator to register 'Friendly signals' in the database and take the the bandscope for subsequent use during the search
- The built-in microphone and correlation modes provide automatic classification of signals according to their danger level in both active and passive (covert) order external antenna. It allows the software to extract signals originating from inside the premises not depending on the kind of transmission, including digital and encrypted protocols

Supplied set

- The DSC-003 controller with USB interface
- The DigiScan EX software (installation package includes driver for the controller)
- The DS-L-AR8200 cable for connection of the AR8200 receiver to the controller
- The DS-L-SND cable for connection of the IC-R(PCR)1500/2500 receiver USB cable
- AC adapter with an additional jack for AR8200

Please note that you will need a communication receiver to be used with the system. Refer to the specification for the list of supplied models. The receiver can be obtained directly from us or a local dealer in your area.



The DSC-003 controller

Optional accessories

- ❶ DS-Line 2 Pro - very-low frequency converter for checking wires (AC 220V, telephone wires, alarm wires)
- ❷ ANT-LINE - antenna for moving away from the laptop computer in order to avoid interference
- ❸ IR-LINE - probe for checking the infra-red range (search of bugging devices transmitting information with the help of IR beams). Connection to the DS-LINE.
- ❹ MLP-LINE - probe for checking the electromagnetic range (checking items for the presence of internal electronics)
- ❺ DS CASE - carrying case for the system
- DS-RM - external reference microphone with a 10m cable. Can be used for checking remote premises. Please note that a built-in reference microphone is already supplied with the system



Specification			
Supplied receivers	AR8200, AR8600, AR5000A, AR8000, SR2200, IC-R10, IC-R20, IC-PCR1000, IC-PCR1500/PCR2500, IC-R1500/IC-R2500 and IC-R8500	Actions performed on detection of a danger signal	<ul style="list-style-type: none"> • Notification to the operator • Marking the signal for report • Automatic sound recording
Frequency range	AR8200: 0.5-3000 MHz IC-R1500/2500: 0.01-3300 MHz Other receivers: please refer to the receiver's specification	Modes of work	<ul style="list-style-type: none"> • 'Pick-up background' - collecting the 'friendly signals' and taking the bandscopes for subsequent use during the search • 'Automatic' - execution of the scheduled task list • 'Manual' - analysis of results of work
Very-low frequency range (with DS-Line 2 Pro converter)	5kHz - 12 MHz plus direct listening	Variants of threshold	Multi-sector threshold, reference bandscope or combination
Kinds of detected bugging devices	In the radiofrequency range: bugging devices installed in a room, car, body-carried, telephone, with autonomous or external power source, FM/AM-modulated, including the spectrum-inverse masking In the very-low frequency range: bugging devices used for transmission: AC wires, telephone/alarm lines or infra-red beams	Kinds of tasks in the scheduler	'Search', 'Analysis', 'Scan Range', 'Scan DB' and 'Frequency watch'
Distance of detection	depends on the transmitter's power and ambient obstacles (5 mW transmitter at a distance up to 100 m)	General radio monitoring functions	Scanning with a random step and mode, programming the resumption conditions and carrying out the sound recording
Speed of scanning (duration of the 50-3000MHz range scanning):	AR8200: not less than 20 min IC-PCR1500: not less than 7 min Other receivers: depends on the model	Sound processing	<ul style="list-style-type: none"> • Automatic sound recording of dangerous signals • Automatic sound recording during execution of radio monitoring tasks with programmable resumption conditions • Audio compression (codecs: MP3, ADPCM, GSM, etc.) • Voice activation with adjustable level and silence interval • Oscilloscope and FFT-spectrograph
Processing of data	<ul style="list-style-type: none"> • Distinguishing signals from the spectrum and splitting them with an analysis of the drop level • Classification of signals by the danger level based on the test results Comparison of levels on the external and the internal antenna in the automatic mode (S-Pro only) 	Database	<ul style="list-style-type: none"> • Format of Microsoft Access (.mdb) • Wide possibilities of operation with the data (filtering, sorting and clipboard) • Generation of reports (printing or saving in the PDF-file) • Export of data into WORD or EXCEL
Performed tests	Passive correlation, semi-passive correlation, active amplitude and spectral correlation, active parametric correlation and harmonic presence test	Connection to PC	USB

DigiScan EX

Counter surveillance sweeping system

Versions of the DigiScan EX

Feature	DigiScan EX Standard	DigiScan EX Professional	DigiScan EX S-Pro
Scheduler	+	+	+
Watchdog timer	+	+	+
Kinds of executed tasks			
'Search' task: searching for listening devices in a specified frequency range, performing tests to estimate a signal's danger level, saving signals in the database (DB) and automatic sound recording on a signal's frequency	+	+	+
Task 'Analysis': testing signals in the DB in order to measure their danger level, automatic recording of sound from dangerous signals	+	+	+
Task 'Scan range': scanning of a specified frequency range with operator-determined step and modulation, saving signals in the DB. Programmable conditions of continuation and automatic recording of sound		+	+
Task 'Scan DB': scanning signals of the DB for their activity, programmable conditions of continuation and automatic recording of sound		+	+
Task 'Frequency watch': watching a frequency for activity, programmable conditions of continuation and automatic recording of sound		+	+
Search features			
Comparison of signals on the external and internal antennas (energetic correlation)			+
Classification of the signals by danger level	+	+	+
Collecting and working with friendly signals to increase speed	+	+	+
Using a reference bandscope as a threshold to increase speed		+	+
Silent search in passive modes	+	+	+
Checking wires for the presence of acoustics in the very low frequency range of 5KHz...2MHz: AC 220V, phone lines, alarms. Checking of the infra-red range is also possible (optional probe required)	+	+	+
Passive amplitude correlation, semi-passive amplitude correlation, active amplitude correlation, active spectrum correlation, active parametrical correlation, harmonic presence test	+	+	+
Automatic recording of sound from dangerous signals	+	+	+
Automatic printing of dangerous signals	+	+	+
Notification to the operator about danger detection	+	+	+
Estimation of the bug's location in 2 dimensions and printout of the results	+	+	+
Monitoring features			
Programmable conditions of the scan suspension and resumption		+	+
Using a reference bandscope as a threshold to increase the scan speed		+	+
Sound recording			
Sound archive stores the frequency, modulation, date/time, duration and DTMF. Automatically erases older sound files when the allowed occupied space is exceeded. Export of sound files is possible.	+	+	+
Bit rate selection (9kHz, 16kHz, 22kHz, 44kHz)	+	+	+
Compression of sound with the help of the following codecs: MP3, ADPCM, GSM, etc. The minimum disk space required for 1 hour is 8Mb (80 Mb without compression).		+	+
Recognition of the DTMF		+	+
Activation by voice with tunable sensitivity and interval		+	+
Database			
Microsoft Access .mdb format	+	+	+
Export of signals to Microsoft Excel or a text file	+	+	+
Printout of signals and their spectrums	+	+	+
Support of banks and filtering by bank		+	+



Global TSCM Group
New York

Global TSCM Group, Inc.

12 W 32nd Street, #604
New York, NY, 10001, USA

www.globaltscmgroup-usa.com
sales@globaltscmgroup-usa.com
+1 212 967 4030

