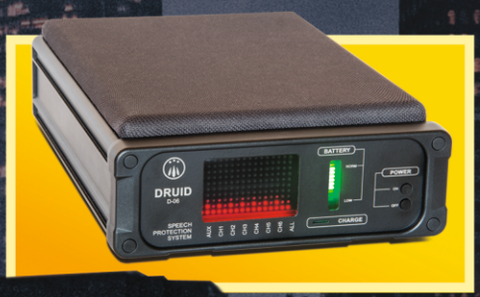
SOLUTIONS FOR COUNTER SURVEILLANCE AND THE PROTECTION OF CONVERSATIONS



WWW.DIGISCAN-LABS.COM

Digiscan Labs.
Securing Information Digitally

PORTABLE DETECTORS

03 iPROTECT 1217

The anti-tracking mobile system, detector of mobile and wireless signals

05 iPROTECT 1216

Counter surveillance 3-band RF detector

06 PROTECT 1207i

Multi-channel detector of wireless protocols

07 iPROTECT 1205

Pen-style RF detector

08 PROTECT 1206i

Detector of bugs and digital transmissions

09 iPROTECT 1215

Microwave pointer

DETECTORS OF HIDDEN VIDEO CAMERAS

i10 WEGA-i

Detector of hidden video cameras

SWEEPING SYSTEMS

i1 DELTA X G2/6,G2/12

Counter surveillance sweeping system

i3 DELTA S

Countersurveillance sweeping system

PROTECTION OF CONVERSATIONS

i5 MNG-300 Rabbler

Mobile noise generator

i6 DNG-2300/DNG-KIT1

Digital white noise generator

i7 TD2300

Vibroacoustic transducer

i7 SP2300

Omnidirectional speaker

i8 DRUID D-06

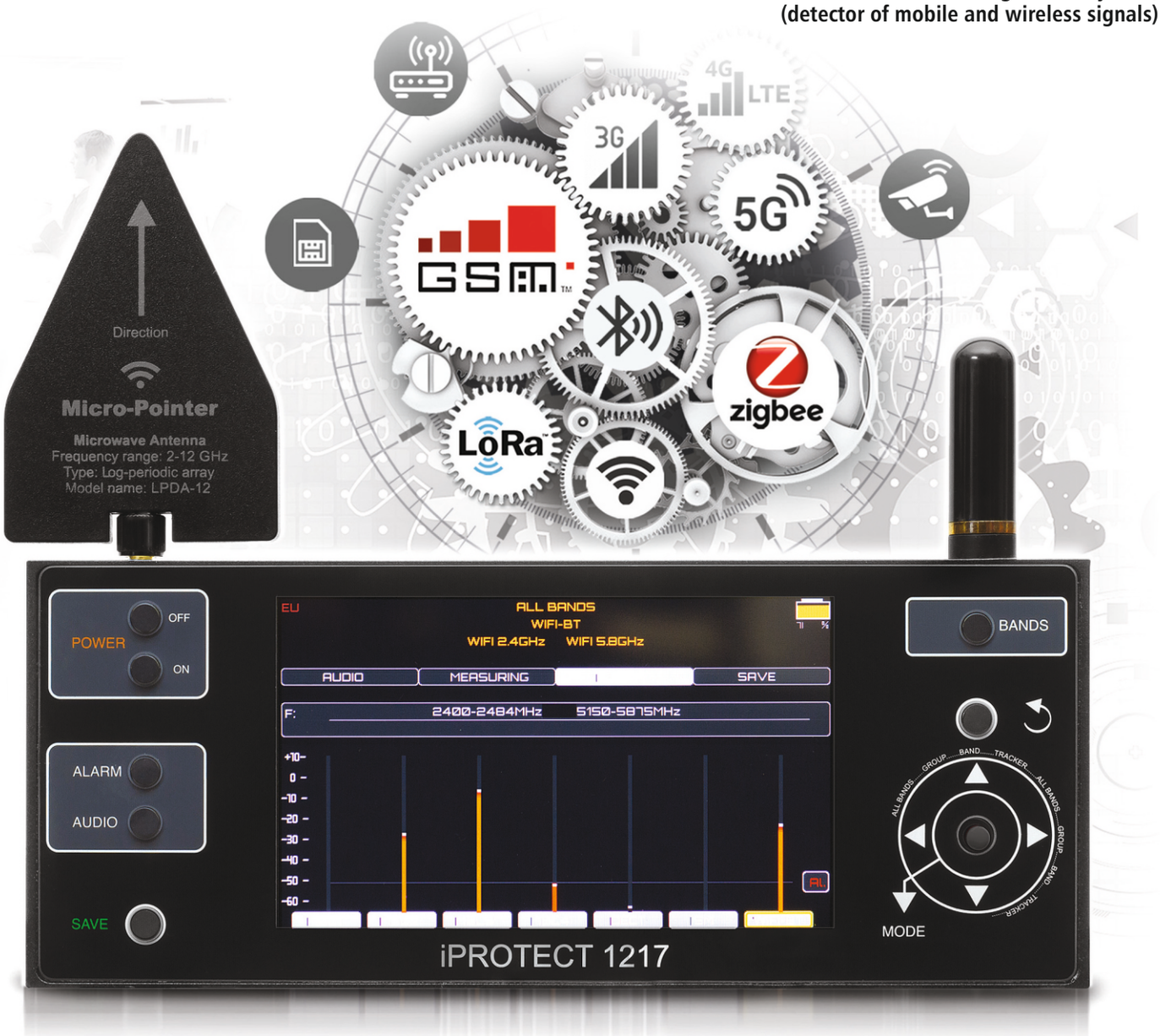
Protection of conversations against all kinds of eavesdropping

i9 PHONE SAFE SUMMIT

Protection against a mobile phone's surroundings listening and recording

iPROTECT 1217

**The anti-tracking mobile system,
(detector of mobile and wireless signals)**



MAIN FEATURES

- Able to detect mobile and wireless signals at a much greater distance compared to convenional RF detectors (at least,10 times more)
- Selective: interference resistant and with a high sensitivity
- Has worldwide coverage of mobile standards – can detect all existing bands of GSM, CDMA, 3G, 4G/LTE and 5G in the range up to 6 GHz
- Able to detect all types of wireless signals,including Wi-Fi 2.4 GHz, Bluetooth, Wi-Fi 5 GHz, DECT, ISM 434MHz, ISM 968 MHz and ISM 915 MHz
- Detection of at least 26 mobile and wireless bands
- Can be adjusted to the frequency allocation of the country of use
- A selective multi-band principle of work informs the user of exactly which signals were found
- The mode of analysis of a certain band facilitates the physical search of a transmitter
- A separate mode for the detection of GPS trackers with history accumulation (TRACKER)
- ALARM function warns the operator about exceeding the threshold, both with sound and visually
- 43 threshold levels for setting optimal sensitivity
- Can be set up for specific tasks, for example, for the detection of Wi-Fi only, etc.
- Operation modes:
  - **ALL BANDS** (detection on all bands)
  - **GROUP** (detection on the selected group of bands)
  - **BAND** (analysis of a separate band)
  - **TRACKER** (detection of GPS trackers)
- Two antenna inputs and two antennas in the set for ensuring maximum sensitivity
- The high-band directional antenna facilitates locating of transmitters above 2400 MHz
- The built-in rechargeable battery provides an operational time of up to 5 hours
- USB recharging

DETECTING OF MOBILE AND WIRELESS SIGNALS

Searching for the illegal use of mobile signals is becoming an increasingly important task during counter surveillance sweeping. It is connected with the numerous means of eavesdropping that transmit information via mobile networks. The mass production of components for developers, such as GSM, 3G, 4G/LTE and 5G modules, enables them to develop cheap and quick surveillance methods which have ultra-high quality of sound, video or location transmission. Hidden cameras camouflaged as household appliances, toys or interior objects, will most likely transmit data via mobile networks or Wi-Fi. Spy listening devices quite often have a slot for SIM-cards for functioning on a cellular network. A GPS tracker is a device that is installed in a vehicle and informs about its location, these also send coordinates via mobile communication.

Unfortunately, wide range RF detectors or near-field receivers have a low sensitivity and are not very suitable for the detection of mobile devices. This is caused by the ability of the RF detectors to receive all signals simultaneously and display them cumulatively on a bargraph, and as a result, stronger signals prevent the detection of weaker ones.

Selective detectors have a much greater distance of detecting mobile signals because they only accept them, and ignore other frequencies. Unfortunately,during the development of a selective detector, one nuance appears. It is very difficult to create a detector able to receive all mobile bands at the same time. As is well known, more and more mobile bands are being used worldwide. The GSM standard works on two bands. Then 3G appeared, occupying one more band. The introduction of the 4G/LTE standard required a wider frequency spectrum for functioning; therefore 3-7 frequency bands were allocated for it in each country. Later still 5G appeared, which requires an even wider spectrum so more wide bands have been allocated for its functioning. Thus, currently, in most countries, there are up to 10-15 different frequency bands of mobile communication according to the national frequency allocation.

It is very difficult to create a selective detector which is able to detect signals from all mobile bands which will work in all countries. Thankfully, the designers of the iProtect 1217 have achieved this. The iProtect 1217 is the only detector in the world which is able to detect all the existing mobile standards on all continents. Its table includes at least 26 bands, which can be selected automatically or manually.

In addition to mobile communication, the 1217 detects signals of Wi-Fi, Bluetooth, DECT, ISM 434 MHz, ISM 868 MHz and ISM 915 MHz. It is well known that these standards can be used by hidden surveillance devices for audio and video signal transmission, and therefore such transmitters must be found and identified.

Apart from a high sensitivity, selective detectors have one more significant advantage compared to wide-band detectors. This is, the user is able to see exactly which signal has been detected. This greatly improves the ability to distinguish suspicious signals from external interferences and enables the user to perform a physical search for a certain transmitter. Such an ability is not available for wide-band detectors which mix up all the signals. The iProtect 1217, as a selective detector, can inspect one separate band, which is why it is irreplaceable during professional searches.

One more important advantage of the iProtect 1217 is the TRACKER mode (searching for GPS trackers). In this mode, the device is adjusted for detecting only mobile signals and accumulates a history for finding the periodic sending of data with coordinates.

SUPPLIED SET

Device	1
High-band antenna Micro-Pointer LPDA-12	1
Low-band rod antenna	1
Charging cable USB Type C	1
Angle adapter SMA	2
A case for transportation	1

SPECIFICATION

Number of bands	26
Antenna inputs	Input 1: SMA, 2400 – 6000 MHz Input 2: SMA, 600 - 2400 MHz
Average sensitivity	-60 dBm
Operation modes	ALL BANDS (detection on all bands) GROUP (detection on the selected group of bands) BAND (analysis of a separate band) TRACKER (detection of GPS trackers)
Alarm function	Visual or audio
Number of alarm threshold levels	43
Sound signals	Alarm, depression of buttons
Regions	US (bands of the USA) EU (European bands) TOTAL (all bands)

Operating and control elements	Joystick: move left-right, up-down, threshold adjustment, mode selection Button POWER OFF: switch off Button POWER ON: switch on Button ALARM: alarm Button AUDIO: sound Button BANDS: band set up Button BACK: exit to the previous mode Button SAVE (storing the current state)
Power supply source	USB 5V
Power	Built-in rechargeable battery 6800 mA*h 3.7 V
Battery operational resource	Up to 5 hours
Weight	The device without antenna: 750 g Packed: 1500 g
Dimensions	The device without antenna: 208 x 86 x 41mm Packed: 27 x 22 x 10 cm
Operating temperature range	-5…50 °C

iPROTECT 1216

Counter surveillance 3-band RF detector

The iProtect 1216 is a new professional RF detector created for discovering all types of RF eavesdropping devices, including analog and digital, as well as those that transmit information over mobile networks and using wireless standards.

KEY FEATURES

3-band detection

The frequency range of the 1216 has been split into 3 parts, each displayed by a separate bargraph: "VHF/UHF 50-700 MHz", "Mobile and wireless 700 MHz – 3 GHz" and "Microwave and wireless 3-12 GHz". The separate indication allows the operator to understand better what type of signal is detected, to detect several signals at the same time and to sustain the ability of detection near the sources of interference.

Microwave

The third "microwave" band of the iProtect 1216 covers the 3-12 GHz frequency range. This band detects Wi-Fi and other wireless protocols operating at 5 GHz and on any higher frequencies. The microwave frequencies are supposed to be more covert since they are not detectable by common RF detectors. The iProtect 1216 finds these signals easily

Alarm

The Alarm feature helps the operator to reject background interference by adjusting the threshold. When a signal exceeds the alarm threshold the device produces an alerting sound. The Alarm is also extremely convenient when probing hard-to-access places or keeping the device in the "guarding" state. The alarm threshold has 48 tuning steps.

Histogram

In the ONE BAND display mode the iProtect 1216 shows the histogram for the selected band in addition to the bargraph. The histogram draws the history of the signal obtained over the last 5 seconds and is very informative when observing intermittent/periodical signals or when probing the area quickly

Wi-Fi and 3G

The iProtect 1216 has a significantly higher sensitivity to the 3G, Wi-Fi and Bluetooth bugging devices compared to conventional RF detectors. This advantage was achieved with the help of the additional radio frequency paths in the circuit dedicated to the specific frequency spans.

Signature

In addition to drawing a bargraph the iProtect 1216 can identify some types of signals and show a corresponding message on the display.

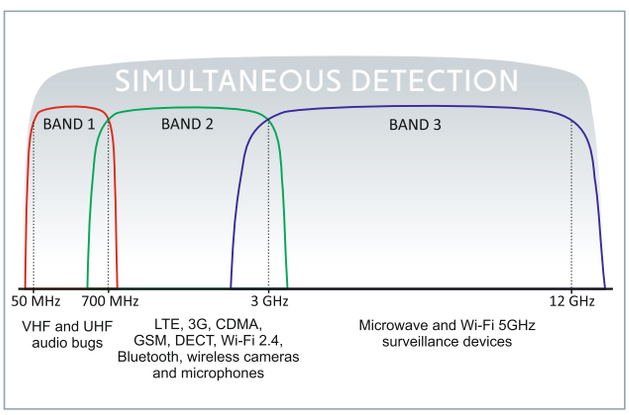
ALL FEATURES

- Detects all types of RF transmissions including analog and digital, audio and video
- Frequency range 50 MHz – 12 GHz
- Separation into 3 bands helps to avoid loss of sensitivity near strong interference
- ALL BANDS and ONE BAND display modes
- High sensitivity to 3G and wireless protocols (Wi-Fi, Bluetooth, etc.)
- Working modes: SILENT, AUDIO and ALARM
- Adjustable alarm threshold
- Portable, reliable and easy-to-use
- The BARGRAPH shows the momentary RF level
- The HISTOGRAM displays the RF signal over 5 seconds (in 'ONE BAND' display mode)
- The SIGNATURE displays the possible signal type
- Built-in directed microwave antenna
- Shock-resistant CNC milled duralumin housing
- Rechargeable Li-Ion battery with resource of 6 hours
- Controlled by microcontrollers
- 2 x built-in OLED displays

SPECIFICATIONS

Frequency range	50 MHz – 12 GHz Band 1: 50 – 700 MHz Band 2: 700 MHz – 3 GHz Band 3: 3GHz – 12 GHz
Indicators	Main display Status display
Display modes	ALL BANDS, ONE BAND
Working modes	SILENT, AUDIO, ALARM
RF connector	SMA (band 1 and 2), 50 Ohm
Microwave antenna	Built-in (band 3)
Threshold settings	48 steps
Battery	Rechargeable Li-Ion 1150mAh@3.7V
Battery resource	6 hours
Recharge time	4 hours
Recharge source	USB
Dimensions with antennas	173 x 71 x 21 mm
Weight	265 g
Operating temperature:	-10° C to 45° C

FREQUENCY COVERAGE



SUPPLIED SET

Detector, rod antenna, mini-USB cable for recharging, user manual

PROTECT 1207i

Multi-channel detector of wireless protocols

The **Protect 1207i** is a 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.

SUPPLIED SET

Detector, 2 Omni-directional antennas, 2 AAA (LR03) batteries, user manual

Detect the following kinds of bugging devices:

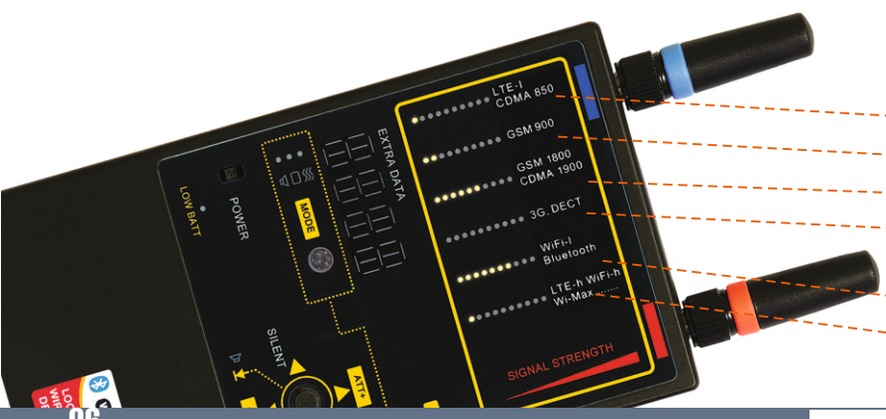
- Bugging devices using GSM/3G/LTE standards
- Spy phones (illegally pre-programmed)
- GPS Trackers
- Alarm systems and baby monitors with 'Listen' function
- Bluetooth bugging devices
- Wi-Fi/Wi-Max bugging devices
- Wireless videocameras 2.4/5.8 GHz

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

iPROTECT 1205

Pen-style RF detector

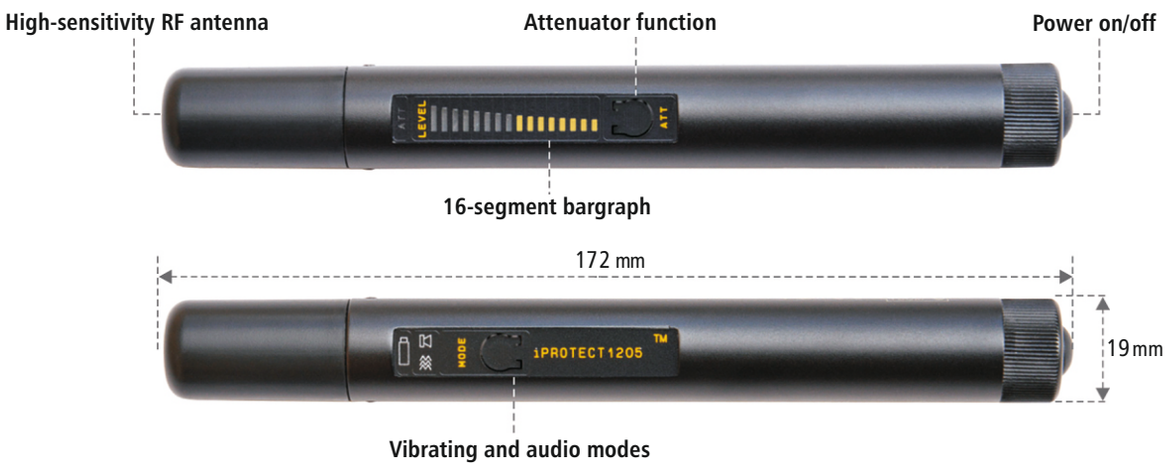
FEATURES

- Easy and quick detection of RF bugs of different types, including VHF/UHF transmitters, GSM bugs, wireless video cameras, Wi-Fi audio and video transmitters, vehicle transmitters, body-carried transmitters, etc.
- 3 working modes: Normal, Vibrating and Audio
- Wide frequency range 50-6000 MHz
- Powered by just 1 x AA battery
- 16-segment bargraph indicator
- Physical attenuator provides the ability to locate strong RF sources
- Highly sensitive to real signals without being affected by weak background radio waves
- No sensitivity loss at battery discharge
- Low power indication
- High-quality detection scheme with professional RF isolation
- Reliable and tested device for different sweeping tasks
- Detects both analogue and digital transmissions
- Allows the operator to locate the source
- Vibrating signal for concealed indication of a high RF level and testing hard to access places
- Durable duralumin case
- Battery resource 10-20 hours

PARTS DESCRIPTION

Designed for simplicity, the iProtect 1205 contains powerful highly-sensitive elements in its circuitry, allowing the operator to conduct countersurveillance sweeping at a highly professional level. The advantage of RF detectors is their wide frequency coverage and their ability to show radio waves right near the source and therefore show the location of the transmitter.

The iProtect 1205 solves this task in the best possible way, accurately eliminating any background noises and indicating real signals. With the help of the 1205 the operator can track all RF sources and is therefore able to find the bugging device if there is one present.



The iProtect 1205 has a16-segment bargraph indicator which allows the operator to see the slightest changes in level and as such accurately find the area with the strongest signal for location.

When it is necessary to decrease the sensitivity, typically during the location process, the operator can use the attenuator function ATT. The iProtect 1205 has a 'physical' (as in professional communications) RF attenuator of a level up to -20dB. The corresponding indicator will show the attenuator status.

The working mode (Vibrating/Audio/Normal) can be selected by the MODE button. The vibrating mode allows the user to 'feel' the increased level without actually watching the bargraph. This is convenient during the process of inspecting hard to access places like gaps under/behind furniture and construction. The Audio mode helps the user to identify signals in many cases.

The power can be turned on and off with the help of the button on the bottom tip of the detector. The battery compartment is also situated there.

When the battery becomes low, the power indicator changes its color from green to orange. When the battery is about to discharge completely, the power indicator becomes red.

The device is powered by 1 LR06 (AA) battery. The resource time is 10-20 hours.

SPECIFICATIONS

Frequency range	50MHz-6GHz
Controls	Power button, Mode buton, ATT button
Indicators	1) 16-segment bargraph; 2) Vibration 3) Battery state (3 colors) 4) Working mode 5) ATT state
Batery recource	10-20 hours
Dimensions	172 x 19 mm
Frequency range	100 mA in stand-by mode 200 mA at a full bargraph
Power source	1 x AA battery (LR06)

SUPPLIED SET

Detector, 2 AAA (LR03) batteries, user manual

PROTECT 1206i

Detector of bugs and digital transmissions

NEW FEATURES

- **New wide-band antenna (for ANT1 socket)**
  Wider coverage, particularly at lower frequencies, has made it possible to increase the detection distance of a conventional VHF/UHF bug by 2-3 times, while saving perfect sensitivity at the higher bands (GSM, 3G, Wi-Fi, Bluetooth, etc.)
- **New Micro-Pointer microwave antenna (for ANT1/ANT2 socket)**
  This is the first time when an affordable RF detector gets the microwave log-periodic directed antenna supplied in the standard set. 2-4 times longer distance to all sources above 2GHz (Wi-Fi 2.4GHz, Wi-Fi 5GHz, Bluetooth, Wi-Max, LTE High, etc.). The directionality provides easy pinpointing of a wireless source. Now you not only know that there is a Wi-Fi source, but can quickly pinpoint it.
- **Increased dynamic range**
  The bargraph now rises quickly to weak signals and increases slowly to strong signals, thus giving the opportunity to locate the source
- **New Attenuator**
  The new algorithm widens the dynamic range even more, making the location procedure easier. Turn on the attenuator near a strong source, the bargraph which lights fully will drop and then increase further, therefore making it possible to locate more precisely.

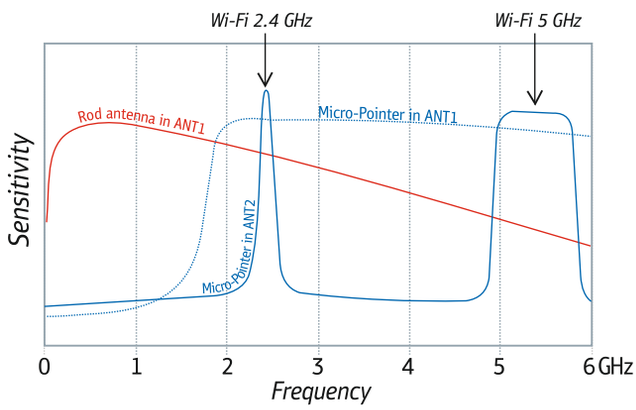
OTHER FEATURES

- Extra high sensitivity to Bluetooth, Wi-Fi 2.4 GHz, Wi-Fi 5GHz and wireless video cameras
- Frequency range:
  - Main antenna ANT1: 50-12000 MHz
  - Auxiliary antenna ANT2: 2.4 - 2.48 GHz, 4.9 - 5.875 GHz
- The perfect tool for searching for digital and analogue transmitters of all types
- 16-segment bargraph indicator
- 3 modes: sound, vibration and mixed
- Correlation function discovers FM-transmitters by the presence of correlation (probing sound is used)
- 2 levels of sensitivity (attenuator)
- Long battery life
- Durable metallic body
- Microprocessor controlled

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, (2.44/5 GHz) 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



Sensitivity graph of the Protect 1206i

SPECIFICATIONS

Frequency range	Antenna 1: 50-12000 MHz; Antenna 2: 2.4 - 2.48 GHz; 4.9 - 5.875 GHz
Power	Two AAA batteries (2xLR 03)
Dimensions	With out antennas: 120x70x16 mm With antennas: 210x70x16 mm
Current consumption	Up to 30 mA
Operation duration	Up to 20 hours
Indications	Active antenna, Low battery, Mode, Identification, Attenuator, Secondary demodulation
Micro-Pointer Antenna	
Frequency range	2-12 GHz
Type	Log-periodic array
Model name	LPDA-12
Dimensions	53 x 84 x 9 mm
Connector	SMA Male

SUPPLIED SET

The Protect 1206i comes with the following accessories:

1 x Rod antenna | 1 x Micro-Pointer antenna | 2 x LR03 (AAA) batteries | 1 x User's Manual

iPROTECT 1215

Microwave pointer

FEATURES

- Detects bugging devices omitted by standard RF detectors
- Discovers microwave signals in the range of 4-13 GHz
- Detects signals not depending on their type – video, audio, digital or analogue
- Built-in directed antenna
- 3 working modes: Normal, Vibrating and Audio
- 16-segment indicator for easy and precise pinpointing of the bugging device
- Sensitivity controlled by attenuator
- Antenna's directivity (out-of-direction attenuation) -6 dBm
- Portable and durable duralumin body
- Powered by just 1 AA (LR06) battery
- Low power indication
- Battery resource 12-25 hours

SUPPLIED SET

Detector, 2 AAA (LR03) batteries, user manual

Conventional RF detectors are typically capable of discovering signals up to 4-6 GHz; therefore higher frequencies usually stay unstudied during sweeping procedures, unless you apply an expensive spectrum analyzer.

The new microwave pointer-probe iProtect 1215 was designed to extend the checked frequency range during sweeping procedures up to 13 GHz.
It can find surveillance bugging devices which are usually not detectable by standard RF detectors. The directed antenna allows the operator to understand where the signal originates from and, as such, to locate the source physically.

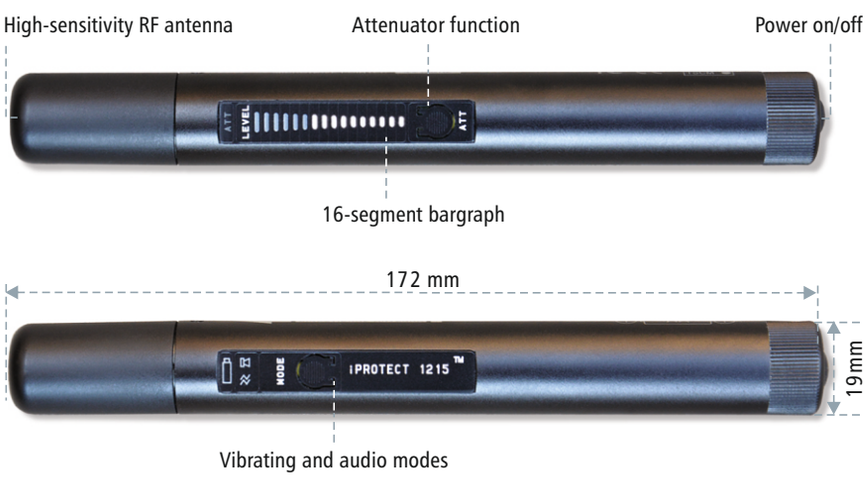
Typical signals detected by iProtect 1215 are:

- Wireless microphones working on 5 GHz frequency band
- Wireless video cameras 5GHz
- Covert 5GHz Wi-Fi access point
- Covert 5GHz Wi-Fi client device
- Other surveillance (bugging devices) employing frequencies between 4-13 GHz

SPECIFICATIONS

Frequency range	4000 – 13000 MHz (4-13 GHz) Power button, Mode button, ATT button
Indicators	• 16-segment bargraph • Vibration • Battery state (3 colors) • Working mode • ATT state
Battery resource	12 – 25 hours
Dimensions	172 x 19 mm
Current consumption	Normal: 80 mA Vibrating: 180 mA Audio: 130 mA
Power source	1 x AA battery (LR06)

CONTROLS



WEGA-i

Detector of hidden video cameras

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 surveilance countermeasures. Thanks to its optical principle the "WEGA-i" can discover lenses of all types of covert cameras not depending on their working state.

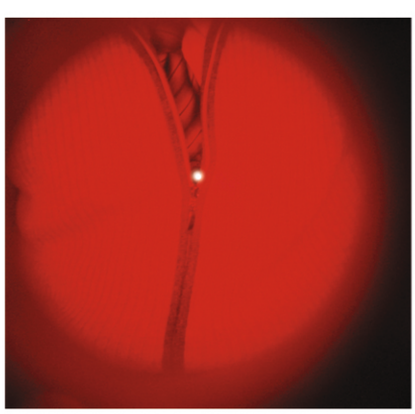
The WEGA's LED matrix radiates a powerful infrared beam which is then reflected by a video camera's optics and is easily detected by the operator.

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.

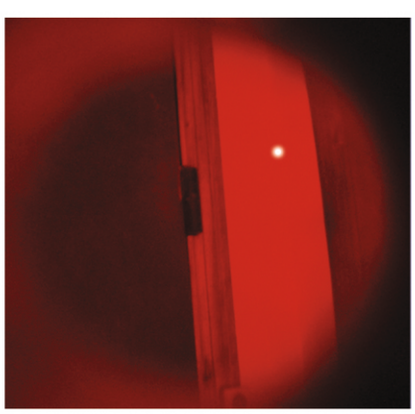
SUPPLIED SET

Detector, 2 AAA (LR03) batteries, user manual

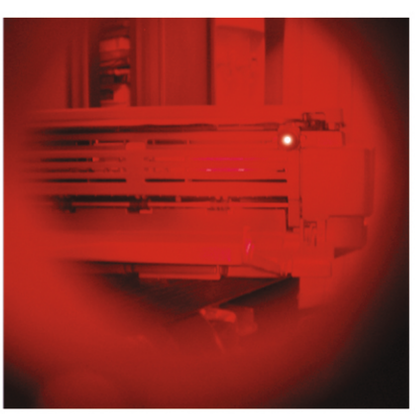
EXAMPLES OF DETECTION



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:

DELTA X G2/6, G2/12

Counter surveillance sweeping system

GENERAL FEATURES

- Both an easy to learn and powerful sweeping system
- Quickly and reliably detects all types of RF surveillance devices in the range up to 6 GHz (12GHz), including analog, digital, working continuously and periodically transmitting audio or video, with or without encryption
- Finds and identifies covert surveillance devices which use the digital standards GSM, 3G, 4G / LTE, 5G, Bluetooth, Wi-Fi, DECT and others in the range up to 6 (12) GHz
- Analyzes Wi-Fi 2.4 GHz, Wi-Fi 5 GHz, Bluetooth, "Bluetooth LE" and "Bluetooth LE Advertising" channels
- Detects RF signal jammers on all bands, including mobile uplinks and downlinks, bands of Global Navigation Satellite System (GPS, GLONASS, GALILEO, etc.), Wi-Fi/Bluetooth, etc.
- Spectral analysis provides high sensitivity and a long detection distance, exceeding the performance of typical RF detectors and near-field receivers by 10-20 times
- The background masking feature allows you to reject friendly signals such as television, radio, mobile base stations, etc., and focus on finding local signals that pose a danger
- Can monitor the RF environment 24 hours a day with full data logging (spectrum traces, alarms). Unlimited number of logs, each can contain an unlimited history of events
- Can be quickly adjusted to the local frequency allocation in the country of use (mobile and wireless bands)
- High-speed spectrum updating and wide real-time bandwidth (RTBW) provide the ability to register short-burst signals
- Search modes include: "All Signals", "Mobile/GPS trackers", "Wireless/ISM", "Downlinks/ Navigation" and "Custom", as well as two additional modes for the inspection of suspicious bands or signals
- Several antenna inputs and a built-in antenna switch provide maximum sensitivity over the entire frequency range·Works with, and is powered by, a laptop or tablet. Is reliably mated with the laptop or tablet in order to be moved during the detecting and locating process. Has convenient magnetic system for attaching the laptop / tablet to the main unit.
- Side handles are used for carrying while all antennas are fixed to the main unit
- Carrying case is in the supplied set

OTHER FEATURES

- "Threat Mark" feature shows dangerous signals on a spectrum graph
- "Burst Hunt" feature improves detection of burst signals such as Wi-Fi, Bluetooth, 5G, etc.
- The audio alarm warns the user about the presence of danger with a sound of variable intensity
- The attenuator simplifies location of powerful transmitters
- The "Hold maximum danger" feature automatically displays the most dangerous band or signal, drawing the operator's attention to the appearance of a threat
- Demodulation of audio in AM/FM mode

COMPATIBLE WITH 12-14" LAPTOPS AND TABLETS

UNIQUE FEATURES of the Delta X

- Wide frequency range:
  Delta X G2/6: 9 kHz - 6 GHz
  Delta X G2/12: 9 kHz - 12 GHz
- Detects illegal information transmission in AC, telephone, Ethernet, alarm and other wires as well as in the infrared range with the help of the supplied Multifunction Probe
- Based on the dBm-calibrated spectrum analyzer providing precise measurements
- Wider dynamic range thanks to the 14 bits bitrate of the spectrum analyzer's ADC
- Alarm indicator on the front panel
- Alarm relay output can activate external devices when a dangerous signal is detected
- The frequency distribution between the antennas can be changed by the operator

ADVANTAGES

Rich selection of search modes

- In the "All signals" mode the system analyzes the spectrum in the full frequency range and detects signals of all types. In addition to mobile and wireless signals, bugging surveillance devices are successfully detected on other frequencies, such as VHF / UHF radio microphones, 900/1200 MHz wireless cameras, and all other RF transmitters up to 6/12 GHz
- In the "Mobile/GPS trackers" mode the system detects mobile devices of all standards, including GPS beacons (trackers) that are installed on vehicles and transmit coordinates via mobile networks. Quickly and reliably detects embedded devices (hidden cameras and microphones) that transmit information via mobile GSM, 3G, 4G / LTE and 5G networks (up to 6/12 GHz).
- In the "Wireless/ISM" mode the Delta X quickly detects Wi-Fi, Bluetooth, ZigBee, DECT, LoRa and other radio frequency devices operating on the ISM bands, such as remote controls, smart home components, wireless sensors, etc.
- In the " Downlinks/Navigation " mode the system scans the downlink bands of mobile networks and bands of Global Navigation Satellite System. With the active "Detect RF jamming" feature the interferences and anomalies created by RF signal jammers will be detected and displayed on the bargraph. Additionally, a special warning sound will be produced.

Handling of bands

- ·Information about the RF environment is displayed on the bargraphs, each responsible for a separate frequency band
- ·By default, the frequency range is divided into several basic bands, in addition to which a number of mobile and wireless bands are added according to the local frequency allocation
- ·The table of bands can be easily adjusted to the frequency allocation of the country of use
- ·It is possible to edit and add new bands, including 4G / LTE and 5G in case of change of frequency allocation

- Each band has an individual threshold which defines the sensitivity and detection distance
- For each band the following information is displayed: name, frequency , current dB level, peak dB level, maximum dB level, threshold, number of dangerous signals and frequency of the most dangerous signal. Additionally , the jammer level is shown when the "Detect RF jamming" feature is active
- The band's bargraph changes color to red when the threshold is exceeded
- The alarm history for each of the bands is stored in the log and displayed on the graph
- The user can inspect separate bands, view the list of signals in it and per form the location of the transmitter

Automatic recognition of signals

- Signals are automatically recognized in spectral traces, added to the signal list, and then automatically updated
- The list of signals is available in the band's inspection mode
- The frequency, band, channel, current, peak, and maximum recorded level are displayed for each signal
- The alarm history for each signal is stored in the log and can be displayed on the alarms graph
- The user can proceed to the inspection of a single signal

Masking of background

- The "Mask Background" procedure allows the operator to collect and mask external signals, such as TV signals, radio signals, mobile base stations, etc. and thus, focus on identifying only those transmitters that are located in the target area.
- Background signals are ignored with the help of the spectral mask, which makes it impossible to hide a bugging device within a TV or radio channel
- This procedure is only required for the "All signals" searching mode
- Signals outside of the mobile and wireless bands are subject to masking only
- The duration of measurement can be selected
- Background masking can be performed at several points around the target zone
- Offset of spectral mask (sensitivity) is set by a threshold

Analysis of Wi-Fi and Bluetooth

- The level of each active Wi-Fi channel is displayed separately when the bands 2.4 GHz and 5 GHz are inspected. Each channel can be studied individually Interferences of Bluetooth are rejected
- Levels of Bluetooth, Bluetooth LE and Bluetooth LE Advertising are displayed separately Each type can be inspected separately. Interferences of Wi-Fi are rejected.
- A list of Wi-Fi access points and not paired BLE devices with their attributes and levels can be displayed in the Devices list and on the spectrum

Threshold and alarm

- Each band has an individual threshold which can be defined by user
- The color of the bargraph changes to red when the threshold level is exceeded
- Signals which exceed the threshold are automatically recognized and stored in the log
- The "Audio alarm" feature warns the operator when the threshold is exceeded. The intensity of the alarm increases as the level rises, which facilitates locating the transmitter
- A full alarm history is stored for each band and signal during the search
- The alarm history of a signal or band can be displayed on the graph for any period

Detecting of RF signal jammers

- Delta X can scan bands where the RF signal jammers may operate - mobile downlinks and bands of Global Navigation Satellite System (GNSS)
- The "Detect RF jamming" feature activates measurement of noise level on all active bands and a special audio alarm
- The feature can be active in all searching modes
- When the presence of an RF signal jammer is discovered, the operator can accomplish finding the source of interference by using the "noise level" bargraph and audio
- In addition to mobile downlinks and GNSS, all other bands can be scanned for the presence of jamming signals

SPECIFICATIONS

Frequency range	**Delta X G2/6:** 9 kHz - 6000 MHZ **Delta X G2/12**: 9kHz – 12000 MHz
Sweeping speed - with Burst Hunt - w/o Burst Hunt	 7 GHz per second 11 GHz per second
ADC resolution	14 bits
Spectrum resolution	9.8 kHz
Unit of measurement	dBm
Sensitivity - standard gain - high gain	 - 85 dBm - 95 dBm
Dynamic range	84 dB
Attenuator	10 dB
Displayed signal level - standard gain - high gain	 -90…-20 dBm -100…-20 dBm (to 0dBm in auto)
Real-time bandwidth (RTBW)	27 MHz
Format	Handheld unit
Platform	Spectrum Analyzer
Antenna inputs	• INPUT: 9 kHz – 3000 MHz • AUX1: 3000-6000 MHz • AUX2: 6000-12000 MHz (G2/12 only)
Searching modes and time of update	• ·All signals (0.9-1.1 s) • ·Mobile/GPS trackers (~0.2 s) • ·Wireless/ISM (~0.3 s) • ·"Downlinks/Navigation" (~0.3 s) • ·Inspect band/signal (~0.1-0.2 s)

Visual elements (panels)	• Level (bands and signals) • Spectrum + Waterfall • Alarms
Demodulation	AM, FM, CW, USB, LSB with bandwidth 2, 5, 15, 50, 100 and 200 kHz
	Intel Core i3 / AMD Ryzen 3 or better (recommended Intel Core i5 / AMD Ryzen 5) 2 USB ports, one should be of SuperSpeed type (USB 3.0/3.1/3.2 or USB Type C) RAM 8 Gb or more SSD 128 Gb or more Windows 10,11 or newer Screen size 12-14"
Powered	by USB-port of laptop / tablet
Battery resource	1-1.5 hour
Duration of work from AC	Unlimited
Displayed spectrum span	1 – 12000 MHz
Peak trace modes	Off, fast, moderate, slow, forever
Range of working temperature	-5°C…+45°C / 23°F … 113°F
Dimensions of main unit (w/o antennas)	33.5 x 26 x 6 cm / 13.2 x 10.2 x 2.4"
Dimensions of packaging	50 x 40 x 20 cm / 19.7 x 15.8 x 7.9"
Weight of main unit with antennas (w/o computer)	3.5 kg
Weight in packaging	10.5 kg

SUPPLIED SET

Item	Delta X G2/6	Delta X G2/12
1. Main unit Delta X	1	1
2. Carry case	1	1
3. USB drive with software and user manual	1	1
4. Omni-directed wideband antenna ODA-4	1	1
5. Microwave antenna MWA-6	1	1
6. Microwave antenna LPDA-12	-	1
7. Multifunction Probe with cables (high-voltage cable, low-voltage cable, 2m coaxial cable)	1	1
8. In-line modular adapter	1	1
9. Set of accessories (adapter USB type C – USB type A – 2; angle USB adapter – 2; magnetic sticker for laptop or tablet – 4)	1	1

DELTA S

Counter surveillance sweeping system

GENERAL FEATURES

- Both an easy to learn and powerful sweeping system
- Quickly and reliably detects all types of RF surveillance devices in the range up to 6 GHz, including analog, digital, working continuously and periodically, transmitting audio or video, with or without encryption
- Finds and identifies covert surveillance devices which use the digital standards GSM, 3G, 4G / LTE, 5G, Bluetooth, Wi-Fi, DECT and others in the range up to 6 GHz
- Analyzes Wi-Fi 2.4 GHz, Wi-Fi 5 GHz, Bluetooth, "Bluetooth LE" and "Bluetooth LE Advertising" channels
- Detects RF signal jammers on all bands, including mobile uplinks and downlinks, bands of Global Navigation Satellite System (GPS, GLONASS, GALILEO, etc.), Wi-Fi/Bluetooth, etc.
- Spectral analysis provides high sensitivity and a long detection distance, exceeding the performance of typical RF detectors and near-field receivers by 10-20 times
- The background masking feature allows you to reject friendly signals such as television, radio, mobile base stations, etc., and focus on finding local signals that pose a danger
- Can monitor the RF environment 24 hours a day with full data logging (spectrum traces, alarms). Unlimited number of logs, each can contain an unlimited history of events
- Can be quickly adjusted to the local frequency allocation in the country of use (mobile and wireless bands)
- High-speed spectrum updating and wide real-time bandwidth (RTBW) provide the ability to register short-burst signals
- Search modes include: "All Signals", "Mobile/GPS trackers", "Wireless/ISM", "Downlinks/Navigation" and "Custom", as well as two additional modes for the inspection of suspicious bands or signals
- Several antenna inputs and a built-in antenna switch provide maximum sensitivity over the entire frequency range
- Works with, and is powered by, a laptop or tablet. Is reliably mated with the laptop or tablet in order to be moved during the detecting and locating process. Has convenient magnetic system for attaching the laptop / tablet to the main unit.
- Side handles are used for carrying while all antennas are fixed to the main unit
- Carrying case is in the supplied set

OTHER FEATURES

- "Threat Mark" feature shows dangerous signals on a spectrum graph
- "Burst Hunt" feature improves detection of burst signals such as Wi-Fi, Bluetooth, 5G, etc.
- The audio alarm warns the user about the presence of danger with a sound of variable intensity
- The attenuator simplifies location of powerful transmitters
- The "Hold maximum danger" feature automatically displays the most dangerous band or signal, drawing the operator's attention to the appearance of a threat
- Demodulation of audio in AM/FM mode

UNIQUE FEATURES of the Delta S

- Frequency range 60 MHz – 6 GHz
- Affordable, lightweight and easy-to-use detecting system
- Fixed frequency distribution between the antenna inputs (INPUT 1: 60 – 2000 MHz, INPUT 2: 2000-6000 MHz)
- High sensitivity and fast scanning speed provides detection of all types of threats

SPECIFICATIONS

Frequency range	60 MHz - 6000 MHz
Sweeping speed -with Burst Hunt -w/o Burst Hunt	 8 GHz per second 10 GHz per second
ADC resolution	12 bits
Spectrum resolution	11 kHz / 21.9 kHz
Unit of measurement	dB
Sensitivity -standard gain -high gain	 -85 dB -95 dB
Dynamic range	72 dB
Attenuator	20 dB
Displayed signal level -standard gain -high gain	 -90…-20 dB -100…-20 dB (to 0dBm in auto)
Real-time bandwidth (RTBW)	24 / 27 MHz
Format	Handheld unit
Platform	SDR by Analog Device
Antenna inputs	INPUT 1: 60-2000 MHz INPUT 2: 2000-6000 MHz
Searching modes and time of update	• All signals (~0.8 s) • Mobile/GPS trackers (~0.2 s) • Wireless/ISM (~0.3 s) • "Downlinks/Navigation" (~0.3 s) • Inspect band/signal (~0.1-0.2 s)
Visual elements (panels)	• Level (bands and signals) • Spectrum + Waterfall • Alarms
Demodulation	AM and FM with bandwidth 5, 15, 30, 100 and 200 kHz (in the range 70-6000 MHz)
Demands on laptop / tablet	Intel Core i3 / AMD Ryzen 3 or better (recommended Intel Core i5 / AMD Ryzen 5)2 USB ports, one should be of SuperSpeed type (USB 3.0/3.1/3.2 or USB Type C), RAM 8 Gb or moreSSD 128 Gb or more Windows 10,11 or newer. Screen size 12-14"
Powered	by USB-port of laptop / tablet
Battery resource	1-1.5 hour
Duration of work from AC	Unlimited
Displayed spectrum span	1 - 6000 MHz
Peak trace modes	Off, fast, moderate, slow, forever
Range of working temperature	-5°C…+45°C / 23°F … 113°F
Dimensions of main unit (w/o antennas)	33.5 x 26 x 6 cm / 13.2 x 10.2 x 2.4"
Dimensions of packaging	50 x 40 x 20 cm / 19.7 x 15.8 x 7.9"
Weight of main unit with antennas (w/o computer)	3 kg
Weight in packaging	8.5 kg

ADVANTAGES

Rich selection of search modes

- In the "All signals" mode the system analyzes the spectrum in the full frequency range and detects signals of all types. In addition to mobile and wireless signals, bugging surveillance devices are successfully detected on other frequencies, such as VHF / UHF radio microphones, 900/1200 MHz wireless cameras, and all other RF transmitters up to 6 GHz
- In the "Mobile/GPS trackers" mode the system detects mobile devices of all standards, including GPS beacons (trackers) that are installed on vehicles and transmit coordinates via mobile networks. Quickly and reliably detects embedded devices (hidden cameras and microphones) that transmit information via mobile GSM, 3G, 4G / LTE and 5G networks (up to 6 GHz).
- In the "Wireless/ISM" mode the Delta S quickly detects Wi-Fi, Bluetooth, ZigBee, DECT, LoRa and other radio frequency devices operating on the ISM bands, such as remote controls, smart home components, wireless sensors, etc.
- In the " Downlinks/Navigation " mode the system scans the downlink bands of mobile networks and bands of Global Navigation Satellite System. With the active "Detect RF jamming" feature the interferences and anomalies created by RF signal jammers will be detected and displayed on the bargraph. Additionally, a special warning sound will be produced.

Handling of bands

- Information about the RF environment is displayed on the bargraphs, each responsible for a separate frequency band
- By default, the frequency range is divided into several basic bands, in addition to which a number of mobile and wireless bands are added according to the local frequency allocation
- The table of bands can be easily adjusted to the frequency allocation of the country of use
- It is possible to edit and add new bands, including 4G / LTE and 5G in case of change of frequency allocation
- Each band has an individual threshold which defines the sensitivity and detection distance
- For each band the following information is displayed: name, frequency current dB level, peak dB level, maximum dB level, threshold, number of dangerous signals and frequency of the most dangerous signal. Additionally the jammer level is shown when the "Detect RF jamming" feature is active
- The band's bargraph changes color to red when the threshold is exceeded
- The alarm history for each of the bands is stored in the log and displayed on the graph
- The user can inspect separate bands, view the list of signals in it and perform the location of the transmitter

Automatic recognition of signals

- Signals are automatically recognized in spectral traces, added to the signal list, and then automatically updated
- The list of signals is available in the band's inspection mode
- The frequency, band, channel, current, peak, and maximum recorded level are displayed for each signal
- The alarm history for each signal is stored in the log and can be displayed on the alarms graph
- The user can proceed to the inspection of a single signal

Masking of background

- The "Mask Background" procedure allows the operator to collect and mask external signals, such as TV signals, radio signals, mobile base stations, etc. and thus, focus on identifying only those transmitters that are located in the target area.
- Background signals are ignored with the help of the spectral mask, which makes it impossible to hide a bugging device within a TV or radio channel
- This procedure is only required for the "All signals" searching mode
- Signals outside of the mobile and wireless bands are subject to masking only
- The duration of measurement can be selected
- Background masking can be performed at several points around the target zone
- Offset of spectral mask (sensitivity) is set by a threshold

Analysis of Wi-Fi and Bluetooth

- The level of each active Wi-Fi channel is displayed separately when the bands 2.4 GHz and 5 GHz are inspected. Each channel can be studied individually. Interferences of Bluetooth are rejected
- Levels of Bluetooth, Bluetooth LE and Bluetooth LE Advertising are displayed separately. Each type can be inspected separately. Interferences of Wi-Fi are rejected.
- A list of Wi-Fi access points and not paired BLE devices with their attributes and levels can be displayed in the Devices list and on the spectrum

Threshold and alarm

- Each band has an individual threshold which can be defined by user
- The color of the bargraph changes to red when the threshold level is exceeded
- Signals which exceed the threshold are automatically recognized and stored in the log
- The "Audio alarm" feature warns the operator when the threshold is exceeded. The intensity of the alarm increases as the level rises, which facilitates locating the transmitter
- A full alarm history is stored for each band and signal during the search
- The alarm history of a signal or band can be displayed on the graph for any period

Detecting of RF signal jammers

- Delta S can scan bands where the RF signal jammers may operate - mobile downlinks and bands of Global Navigation Satellite System (GNSS)
- The "Detect RF jamming" feature activates measurement of noise level on all active bands and a special audio alarm
- The feature can be active in all searching modes
- When the presence of an RF signal jammer is discovered, the operator can accomplish finding the source of interference by using the "noise level" bargraph and audio
- In addition to mobile downlinks and GNSS, all other bands can be scanned for the presence of jamming signals

SUPPLIED SET

Item	Delta S
1. Main unit Delta S	1
2. Carry case	1
3. USB drive with software and user manual	1
4. Omni-directed wideband antenna ODA-4	1
5. Microwave antenna MWA-6	1
6. Microwave antenna LPDA-12	1
7. Set of accessories (adapter USB type C – USB type A – 2; magnetic sticker for laptop or tablet – 4	1

MNG-300 Rabbler

Mobile noise generator

FEATURES

- Was designed by TSCM/countersurveilance 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 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 Rabbler 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 **MNG-300 Rabbler**
  - 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 Rabbler 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, orimpossible, to extract the speech component. Since the generator createsa '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 Rabbler 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

Please note that the MNG-300 Rabbler 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 Rabbler 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.

SPECIFICATIONS

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

SUPPLIED SET

Generator, 1x 1604A (6LF22) battery, user manual

DNG-2300/DNG-KIT1

Digital white noise generator

FEATURES

- Creates powerful protection against the leakage of all types of vibro-acoustics by injecting non-filterable noise into surrounding structures and cavities
- Suppresses wall contact microphones, window laser systems and wired microphones inside walls, voids and ventilation shafts (air ducts)
- Is a key part of the protection system which also includes wire-connected transducers and speakers
- Generates white noise – the output interference is evenly distributed through the spectrum of a human's voice
- Has 3 independent output channels: 2 x TRANSDUCERS and 1 x SPEAKERS
- All 3 channels have individual level adjustment
- Each TRANSDUCERS channel can feed up to 12 transducers mounted on solid structures (concrete/cement/bricks) and up to 24 transducers on light structures (glass, pipes, drywall, wood)
- The SPEAKERS channel can feed up to 12 speakers
- The MUTE control input allows the user to turn off the speakers temporarily

VIBRO-ACOUSTIC EAVESDROPPING

It is well-known that sound permeates through walls, doors, water, windows and other constructions as well as through voids, cavities and ventilation shafts. This property of materials makes it possible to intercept conversations conducted within a premises with the help of highly sensitive contact microphones (electronic stethoscopes), window laser systems or conventional microphones without entering the target area.

Wall contact microphones can pick up vibrations from the plumbing, structures, walls, windows, doors, floors, ceilings and more. The listening device may be in an adjacent room, or even several floors or rooms away attached to a wall, pipe or other fixture. Cavities such as air ducts, ventilation shafts or other voids can be used for intercepting sound from an adjacent premises with a help of conventional microphones.

Window laser systems are able to "read" conversations from the premises by sending visible, or nvisible, nfrared beams to the glass and extracting the sound vibrations from the reflected rays.

The DNG-2300 generator, together with its transducers and speakers, counteracts all the above mentioned methods of listening by creating powerful, non-filterable interference on the structure of a building and within its voids. While transducers inject their generated noise into surfaces and structures, stopping the distribution of sound through them, the role of a speaker is to fill voids, cavities and ventilation shafts with audio interference to prevent leakage of sound through the air.

DNG-2300/DNG-KIT1

Digital white noise generator

● DNG KIT1

● standard set

SPECIFICATIONS	
Power source	110-220 V, 50-60 Hz
Dimensions	6 x 17,5 x 25,4
Weight	2.2 kg
Output channels	2 x TRANSDUCERS 1 x SPEAKERS
Peak output voltage	12 V
TRANSDUCERS output (2)	
Max. output power	2 x 10 W
Frequency response	180-5600 Hz
Minimal impedance of load	3 Ohm
Recomended transducers	TD 2300
Max. quantity of transducers per channel	24 (light structures) 12 (solid structures
SPEAKERS output	
Max. output power	1 x 8 W
Frequency response	180-7000 Hz
Minimal impedance of load	8 Ohm
Recomended speaker	SP 2300
Max. quantity of speakers	12

SUPPLIED SET	DNG KIT1	standard set
Noise generator DNG-2300	1	1
AC power cord	1	1
Transducer TD2300 4 Ohm	12	-
Speaker SP2300	2	-
Carry case	1	-

TD2300

Vibroacoustic transducer

The TD2300 vibroacoustic transducer is part of a complete counter surveillance protection system. It inducts noise into walls, floors, ceilings, windows and other surfaces of the building, preventing leakage of sound signals. To provide a sufficient level of protection the system consists of a number of transducers installed on different structures in the room and is connected to a generator

ADVANTAGES

- Attractive design, looks good in any interior
- High power output, combined with compactness
- Fits equally well on windows, walls and other structures
- The included mounting set makes it possible to install the transducer on any surface
- Passes most of the generated noise into the desired construction in the form of vibration, while also producing less audible interference
- The frequency characteristics optimally correspond to the spectrum of human's speech
- Perfectly suited for the DNG 2300 white noise generator

SPECIFICATIONS	
Impedance	4 Ohm
Frequency response	58 Hz -12 kHz
Power	10W
Weight	252 g
Dimensions	56 x 27 mm

SP2300

Omnidirectional speaker for white noise generators

The SP2300 omnidirectional speaker is part of a complete counter surveillance protection system While transducers inject their generated noise into surfaces and structures, stopping the distribution of sound through them, the role of the speaker is to fill voids, cavities and ventilation shafts with audio interference to prevent leakage of sound through the air.

Prevents the following ways of listening:

- Listening with the help of a wall stethoscope placed behind the construction which is adjacent to a cavity in the room (typically from the floor above, behind a dropped ceiling)
- Leakage of sound outside the target room through voids/cavities (for example, through ventilation shafts or common holes for the pipes of a heating system)
- Placing a wired microphone in a void or cavity
- Hiding a covert surveillance device in a void or cavity

SPECIFICATIONS	
Power output	9W (3 x 3W)
Resistance	24 Ohm
Dimensions	110x80 mm
Weight	360 g

DRUID D-06

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.

SUPPLIED SET

1 x charger/power supply, 6 x headsets, 1 x carry case, user manual

Supplied set

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
- 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

Headset for DRUID D-06

SPECIFICATIONS

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

PHONE SAFE SUMMIT

Protection against a mobile phone's surroundings listening and recording

Obviously mobile phones have an infinite number of benefits for communication and business; however, they also create certain threats of information leakage. One of the potential leakage channels is the phone's microphone being able to pick up surrounding acoustics with a high sensitivity.
The PHONE SAFE SUMMIT has been developed by information security professionals to protect against this exact type of threat.

While developing this product the following features and vulnerabilities of modern phones were taken into account:

- The phone can be intentionally, or covertly, 'off-hook' during important negotiations
- Voice recording software can intentionally, or secretly, run on the smartphone
- Listening software can run in a 'stealth' mode
- Spyware can be installed on the smartphone without the owner's knowledge, allowing attackers to activate covert eavesdropping around the phone. There are known cases of transmission of such software by exploiting the vulnerabilities of some messengers
- The acoustic environment around the phone can be transmitted to the server, or cloud service of the attackers either in real time or with a postponed uploading
- Smartphone apps which have access to the phone's microphone can be used for eavesdropping in cases of them having been hacked (usually messengers or social network apps)
- Uploading of information can be done in the following ways:

CONVENTIONAL VOICE CALL | **MOBILE INTERNET** | **Wi-Fi** | **BLUETOOTH** | **THE PHONE'S CONNECTOR**

Unfortunately, the creation of radio interference (RF jamming of mobile communications, Wi-Fi and Bluetooth) does not guarantee protection, as there is still the possibility of accumulating information in the phone's memory (voice recorder mode). Given this factor, the only reliable way to protect is to block the phone's acoustic channel. This prevents acoustic information from leaking, regardless of how it is listened to or transmitted. A number of modern technologies have been used in the **PHONE SAFE SUMMIT** device for your protection.

FEATURES AND ADVANTAGES

- Blocks the microphone of the phone with the help of non-filterable inaudible ultrasonic interference
- Efficiently prevents surround recording app from capturing conversations and sounds
- Suppresses both the bottom and upper microphones of the phone by creating two-side interference
- Up to 4 phones can fit inside
- Inaudible frequency of interference has been optimally selected for the best performance and affects all existing models of smartphones
- Made with the design of an attractive natural wood stand
- The acoustically isolated phone can remain close to the owner where the screen can be easily observed
- The phone stays online and available for incoming calls
- No illegal radio jamming
- Can be powered by the external USB, or from the built-in rechargeable battery
- Has 2 sensors, increasing the battery's resource: the device starts producing interference when a phone is inserted (IN USE sensor) and a conversation is present (ACTIVE sensor)
- Is compatible with all types of phones (max. height 180 mm)

SPECIFICATIONS

INTERFERENCE	
Type of interference	Ultra sound, inaudible frequency
Power of noise	<2 W in the active area
DIMENSIONS AND WEIGHT	
Dimensions (width x height x depth)	262 x 78 x 82 mm
Compatible phones	Height up to 180 mm
Weight	600 g
POWER	
Source	1) USB 5V 2) Built-in rechargeable battery
Current consumption	500 mA (noise mode) 6 mA (stand-by mode)
Battery	Li-Ion, 3.7 V, 6800 mAh
CONNECTOR	USB Type C
Battery resource	> 10 hours
Recharging time	12 hours
OTHER	
Sensors	IN USE , ACTIVE
Indicators	BATT, ACTIVE, IN USE
Capacity	Up to 4 phones

SUPPLIED SET

Device, USB-C, charging cable

WWW.DIGISCAN-LABS.COM

Find a dealer in your country