PROTECT 1207i

Multi-channel detector of wireless protocols

PROTECT 1207i

Multi-channel detector of wireless protocols

USER MANUAL

LOCATES WIRELESS DEVICES

DETECTS GSM/3G BUGS AND TRACERS

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/LTE
- Detection of Bluetooth/Wi-Fi/WiMAX
- 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

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
WiMAX/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 x16 mm
Weight	217 g

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 WiMAX. 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.

It is recommended that all sources of RF waves are detected in the premises during a search. It is necessary to determine the nature of every source - whether it is a regular transmitter like a Wi-Fi access point or it has an unclear origin and thus should be inspected and probably removed.

Ways of eavesdropping

The following are the most probable ways of eavesdropping with the use of wireless protocols:

GSM/WCDMA/3G/LTE

GSM baby-monitor/GSM alarm/GSM bug

A small box with a SIM-card insert. Can transmit acoustics or conversations from a landline telephone to a pre-programmed number via the GSM network. Can be controlled form a pre-programmed number with the help of SMS or programmed from a PC. It is powered from a mains supply and has its own rechargeable backup battery.

GSM/GPRS/EDGE/3G/LTE video camera

Has a built-in video camera and can transmit captured still images, video and acoustics. It is usually used for security observation but can also be used for illegal bugging. On the GSM network still images can be transferred with the use of GPRS/EDGE, but 3G allows for the passing of real-time videos.

Spy phone

A cellular telephone converted into a 'spy phone' with the help of special, illegally installed software. The software allows the illegal listener to activate the microphone of the telephone and transmit acoustics to a pre-programmed number. The control of this device is accomplished in a similar way - by SMS or from a PC.

GPS tracker

A small device which can be installed in a target's car or hidden among their items for personal tracing. Detects its own coordinates with the help of a built-in GPS receiver and then transmits them with the help of the GSM/3G network or can record a trace into its built-in memory. Most of these devices also have a built-in microphone and allow the operator to listen to acoustics in addition to knowing its coordinates.

Bluetooth

Bluetooth bugging device

A small device which is only limited in its size by the desired battery source. If provided with an external power source these devices can achieve a size of 1x1x0.5 cm. They are hardly detectable due to:

1) low power, non-constant transmissions at relatively high frequency ranges; 2) the possibility of remote deactivation thanks to the duplex possibility of Bluetooth; 3) The possibility of gathering information, holding it and then transferring it by remote inquiry during night time - this means that no radio waves are sent during working hours; 4) its small size.

Spy phone

Similar to GSM, the acoustics around the telephone can be picked up and transmitted via Bluetooth if the telephone has special 'spy' software pre-installed.

Wi-Fi/WiMAX

Wi-Fi bugging device

Can transmit acoustics or high quality videos using the standard wireless network. The information can then be easily forwarded onto the Internet and monitored from anywhere in the world. Controlling the device can also be done via the Internet.

Spy phone

Again, having pre-installed 'spy' software in a mobile phone with Wi-Fi (i.e. a Smartphone) allows the eavesdropper to listen to the surrounding acoustics in real-time or they can initiate the downloading of pre-captured data.

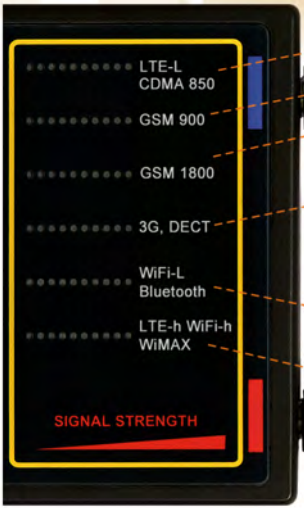
WiMAX bugging device

In addition to the possibilities provided by Wi-Fi, WiMAX gives direct Internet access and a longer coverage distance. This can give the eavesdroppers practically unlimited possibilities in monitoring and control, including transmitting of acoustics, real-time video, remote controlling, collecting information with a fast transfer time, etc.

The Protect 1207i has been designed to detect all of the mentioned kinds of bugging devices.

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 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 2.5-6GHz, including most kinds of the WiMAX/Wi-Fi High/LTE (4G) protocols

The closer the unit is to the source of transmission the higher the bar graph level will be. Some powerful sources may cause full illumination of the display (this also happens when the unit is in close proximity to a transmitter). In such cases use the attenuator function (ATT +/ ATT- buttons) to alter the sensitivity.

It is also recommended to use the attenuator when there are many background noises in the area which can create difficulties before a search. Please note: The vibration function will turn on when the SIGNAL STRENGTH of any of the bar graph indicators approaches the level selected in the setup mode.

Joystick controls and operation mode

The right arrow on the joystick control of the Protect 1207i is used for selecting the desired indication method. There are four modes available:

- Silent - used in most cases for covert operation. The operator should watch the bar graphs in this mode
- Listen mode, when the unit's speaker produces a demodulated signal
- Visual mode, when the unit tries to recognize what protocol is being transmitted in the current signal and shows the results on the 'EXTRA DATA' display.
- Vibration, in this mode the unit's vibrator turns on when reaching the threshold of any of the 6 bar graphs (the threshold can be selected in the setup mode)

The Vibration mode is convenient when probing difficult to reach objects and places. The operator can work without the necessity of watching the bar graphs a high RF level will be indicated only by the Protect 1207i's vibration.

The Visual mode can be turned on when help is needed in detecting what kind of protocol is being transmitted in the near vicinity. The 'EXTRA DATA' display will show the results in this case.

The Listen mode is convenient for a fast search as an experienced operator may be able to distinguish between different types of signals. (Please note that this mode is not suitable for covert searches, as the transmitter will 'hear' sounds in the room.)

The left arrow of the joystick returns the unit to 'SILENT' mode.

Pressing the joystick's button will turn on the Listen mode temporarily

Setup mode

Press and hold the joystick's button and then turn the Protect 1207i on. Use the arrow up or down to select the threshold level for vibration. After this procedure has been completed press the joystick's button to start normal operation.

Power

The Protect 1207i is powered by two AAA (LR03) batteries. It is recommended to use alkaline batteries in order to reach optimal working duration. The 'LOW BATT' indicator will turn on when the batteries are nearing exhaustion.

Usage

Sweeping the room

Please note that the Protect 1207i is an auxiliary device which detects communication protocols only. For full, irrefragable results the premises or vehicleshould be swept with a number of different types of equipment, including wide-band RF detectors, radio-monitoring scanning systems, non-linear junction detectors, video-camera detectors, thermal vision devices, etc.

A wireless detector is an additional but irreplaceable component for such a professional kit and due to its qualities the Protect 1207i is the best selection.

Before starting sweeping, some preparation tasks should be carried out. Firstly, it is necessary to consider the time and individual circumstances of the sweep. Due to there being lots of devices which are remotely controlled it is recommended to carry out a sweep during working hours in real situations when the eavesdropper most wants to listen. It may be necessary to arrange a fictitious meeting. Nobody has to know about the pending search.

Close all drapes in the room. Turn on all the lights and activate any other devices to imitate normal conditions. It is also advisable to turn on a source of sound such as a stereo system or radio. This sound source has two very important functions:

- Voice activated transmitters will be activated
- Your actions will be masked

To avoid false detections turn off all RF transmitting devices before starting the sweeping procedure:

- Wi-Fi routers and Wi-Fi devices (printers, video cameras, laptops, etc.)
- Cordless phones
- Cell phones
- Bluetooth devices, etc.

1. Enter the room and turn on your Protect 1207i. Watch the bar graphs and if they show increased levels (more than 4-5 segments), turn on the attenuator by shifting the joystick in the upper direction (ATT+). The corresponding LED will show the attenuator has been turned on. Note: Later you can turn off the attenuator by pushing the joystick in the opposite direction.
2. Choose the operation mode by sequentially shifting the joystick to the right:

- **Silent** - the default mode which is automatically selected after turning the unit on. It can also be selected in the sequence of modes (joystick right) or chosen quickly by shifting the joystick to the left. This mode is useful when a covert procedure is necessary.

- **The Listen mode** is more convenient for locating and inspecting the RF source as the operator can learn about the source by hearing the demodulated signal. An experienced operator may be able to distinguish between different kinds of transmission:
    - Bluetooth gives a 'crackling' sound
    - Wi-Fi will produce a 'scratching' sound
    - GSM gives a 'buzzing' (hum)
    - DECT is heard as an AC transformer hum

  Note: The above is a guideline only as the sound may vary depending on the current mode of transmission and the type of the protocol used in the specific country.
  The Listen mode can be turned on temporarily from any mode by pressing and holding the joystick's button.

- The Visual mode gives extra information to the operator by showing a suggested protocol on the display. The recognition is based on analyzing the demodulated signal and is in most cases sufficiently accurate. Enter this mode when inspecting the RF source.

- The Vibration mode allows the operator to avoid constantly watching the bar graphs when inspecting areas that are difficult to access, and to achieve secrecy during a sweeping procedure. By default the vibration turns on when a constant signal has reached a bar graph level of 5. You can use the Setup mode to change this threshold: Firstly, turn off the Protect 1207i by pressing and holding the joystick's button, then turn the unit on again in the normal manner. Use the up/down arrow to select the desired threshold level of vibration. After this procedure has been completed press the joystick's button to start normal operation.

3. Move around the room with the Protect 1207i while watching its bar graphs or paying attention to the vibrator. Turn the lights and other equipment in the room on and off. Walk around the room, continuously watching the indicator or feeling for the Protect's vibration. The bar graph level will increase or decrease when the detector is closer to, or farther away from a transmitting device.

Probe all objects which may contain a hidden surveillance device. When you get close to an RF transmitting device some of the bar graphs of your Protect 1207i will rise (or the vibration will appear).

The distance of detection may vary depending on the situation. Usually the Protect 1207i is able to detect a GSM 'bug' at a distance of 2-10 meters and a Bluetooth channel at 50-150 cm, although it is recommended to probe objects at a closer proximity 10-30 cm.

The bar graphs can display 10 different levels. You can use the attenuator to decrease the sensitivity when performing the location procedure (finding the source of the RF field). Use the ATT+ arrow when the bar graph shows a high level to force the unit to react to a stronger field only.

Please note: If you want to continue sweeping after the location of one bugging device, it may be necessary to restore the normal sensitivity of the Protect 1207i by using the ATT- arrow.

4. If you have found a source of wireless transmission inspect it very carefully to detect if it is a 'legal device'. Consult IT employees to become acquainted with the scheme of wireless access points and the location of wireless telephones used in the office.

   Illegal transmitters have a number of typical signs, they are:
   - Compact
   - Hidden
   - Handmade or produced with low quantity
   - Contain microphones or video cameras
   - Implanted inside another piece of electronic equipment
   - Connected to a telephone line
   - Connected to AC wires or with its own source of power
   - With an antenna
   - With a SIM card inserted
5. Regardless of the results, apply all other sweeping devises available and carry out a physical search. Visually inspect and probe each object in the highlighted area. Disassemble, if necessary, lamps, desktop items, telephones, AC outlets, phone outlets. Inspect all power and phone lines carefully. Open books, wardrobes, etc. Please remember, that a physical search is a fundamental operation during a sweep.

   If you find a bugging device, do not stop! You should continue the

search more carefully as eavesdroppers often install more than one device. They may install a so called 'foolish bug' which may be easily detected and some other well hidden devices that may have remote control and non-standard modulation.

Checking telephone lines

When talking about phone lines we should firstly mention GSM/3G/LTE (4G) bugging devices, which can pick up conversations from a normal landline telephone and then transmit them via the GSM/3G/LTE(4G) network. It is also probable that a Wi-Fi/WiMAX or Bluetooth channel can be arranged to transmit the information.
The Protect 1207i has been specially designed to detect all of the mentioned kinds of telephone bugging devices.

Telephone bugs may be installed anywhere a phone line lays. It may be within the phone set, the phone outlet, connecting box or cable. Most telephone bugs activate only when the receiver is off-the-hook.
Therefore the sweeping of phone lines should be carried out only when the receiver is in this state. Start checking from the phone set itself.
Place the Protect 1207i near the set and lift the receiver. Watch for an increase of the RF level (or starting of the vibration). (Please note: It is pointless to test wireless (radio) telephones, for they act exactly like a bugging device themselves due to the use of radio waves. Only a physical inspection of these items is sufficient to know if they are bugged.

Move the detector along the phone line while keeping the receiver off-the-hook. Check all the outlets and communication boxes. If possible ask a second person to lift the receiver and then hang it up repeatedly. If you see that the RF level changes when the line is activated and deactivated, this is a sign of a bug's presence. Try to locate the place where the RF level is highest and then perform a physical search.

Testing people

The Protect 1207i can be used for detecting the following bugs carried on people:

- Mobile phones, set up in the listening mode (intentionally by establishing a call or secretly with the help of the 'spy software')
- Bluetooth transmitters (real listening devices or conventional Bluetooth devices converted into bugs - headsets, headphones, etc)
- Personal GPS trackers

- Different kinds of listening and watching devices using communication protocols for transmission

Testing procedure

If necessary turn on the attenuator. While carrying the Protect 1207i, approach the person. An increased level on a bar graph will show activity at the corresponding range, which can mean the person has a transmitting device. If you change location you will need to select the necessary attenuator mode in accordance with the background noise.

Another way of testing people is to place the Protect 1207i on the desktop and watch the bar graphs carefully when the person approaches the table and sits down.

How to detect GPS trackers using the Protect 1207i

There are 2 methods to detect GPS trackers using the Protect 1207i:

1. To detect transmissions (uploads) going from the tracker to the mobile network GSM/3G when the vehicle is moving
2. To detect the reestablishment of the connection between the tracker and the network after the connection was lost

Method 1

The Protect 1207i can detect GPS trackers when they transmit their coordinates. Many trackers have a vibration sensor (G-sensor) and do not send coordinates when the car is not moving. The transmissions can be made with a pre-programmed interval, for example each 15 seconds, 1 minute or 15 minutes. It is also possible that a tracker uploads the collected coordinates under an external request and does not initiate transmissions by itself. Therefore Method 2 is better, although extra equipment is needed.

A) Make sure your own mobile phones are off ('flight mode' on or power off) and there are no other phones in the car. If the car has its own GSM/3G phone or an anti-theft alarm system, it is necessary to deactivate the phone or alarm system by taking out its SIM card temporarily

B) Position the Protect 1207i in a front part of the vehicle and start moving. If possible, select a route far away from highly populated cities (in the country) in order to avoid accidental measurements of GSM/3G signals from other peoples' mobile phones.

C) Watch the GSM and 3G bargraphs on the Protect 1207i. Typical periodical increases might be a sign of the tracker sending signals to the network. As it was said above it is unknown what interval can be pre-programmed in the tracker, but it should be the same during the measurement. So, if you observe increases on the bargraph with a non-changing interval, it might be a sign of the presence of a tracker

D) The vehicle should be moving during the measurements. For an 'express' variant 30 minutes of testing might be enough, for a 'deep seeking' drive for 1-2 hours while watching the detector.

E) Repeat the procedure with the Protect 1207i placed in a rear part of the car as it is unknown in what part of the car the tracker might be hidden.

Method 2 (recommended)

This method is more reliable, since it helps to detect trackers even if they are programmed not to transmit the 'route' but to collect it in the memory for a future upload under request. This method detects the GSM/3G modules built into the trackers, forcing them to communicate with the network. To apply Method 2 it is necessary to have a portable GSM/3G jammer with an output power not less than 1W per range (GSM900, GSM1800, 3G – not less than 3W total). But a higher power will give more reliable results.

The mobile network consists of a number of LACs covering the territory. When the phone (or GSM/3G module in the tracker) is changing the LAC, it re-registers in it (location update). The size of LAC may vary depending on the load on the mobile network, but typically if you drive through the city 10-15 km in one direction, you will enter another LAC.

A) Turn on the GSM/3G jammer in your vehicle and make sure it is working - your own telephone should be jammed (sign 'no network')

B) Turn off all the telephones which are in the car ('flight mode' on or power off). If the car has its own GSM/3G phone or an anti-theft alarm system, it is necessary to deactivate the phone or alarm system by taking out its SIM card temporarily.

C) Watch the Protect 1207i' bargraphs to check that the jammer is working (full level).
D) Drive to another LAC (10-15 km away) and stop your car where no other phones can be present (i.e. not in a crowded place)
E) While watching the Protect 1207i' bargraphs turn off the jammer. The levels on the bargraph should drop instantly. If after the decrease they again show impulses of 1-3 seconds duration, it means that there is a GSM/3G device nearby. Such increases are a sign of a tracker.
F) To have a more reliable result you can repeat the procedure by returning to the initial place with the jammer again turned on but placed in another side of the vehicle, for example in the rear. When you arrive, place the 1207i in a rear part too before turning off the jammer.

Before testing your vehicle for trackers, you can check that you are using the correct point of measurements and there is another LAC in the area. Use your own phone, leave it turned on, drive with the jammer turned on, then turn off the jammer and check with the 1207 if your phone starts exchanging with the network (increase 1-3 seconds).

[i] Location Area Code (LAC) is used to identify different location areas. When the mobile station is moving and enters the new location area, it registers itself there in order to receive incoming calls.

Other applications

If you cannot inspect a whole room, for example, in a restaurant or some-one else's office, the Protect 1207i can be used for checking the closest objects to you. In a restaurant it may be necessary to check the items on the table, or the table itself, since they can contain a bugging device.

Detection distance

The detection range of the Protect 1207i depends on two major factors:

- The output power of the transmitter
- The surrounding RF environment waves radiating from other communication devices acting on the frequencies being inspected by the Protect 1207i.

The level on the display of the Protect 1207i will increase as you approach an RF source (or the vibration will start). Either a surveillance transmitter or a safe signal (background noise) can cause it to increase. Successful location of a hidden bugging device is accomplished by finding the area which produces the highest level on the bar graph of the Protect 1207i. Normally the Protect 1207i is able to detect a CDMA/GSM/3G/LTE(4G) signal at a distance of 2-10 meters and Bluetooth / Wi-Fi / WiMAX /DECT channels at 50-250 cm.


PROTECT
1207i