Introduction

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, Wi-Fi, GSM and DECT. 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 'classical' bugs and inspect them for the presence of correlation by sending sound impulses.

Main features

- Detection of Bluetooth, Wi-Fi, DECT and GSM900/1800
- The perfect tool for searching for digital and analogue transmitters
- Frequency range:
  - Main antenna 50-4000 Mhz
  - Auxiliary antenna 2.44 GHz
- 6-segment bar graph 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)
- Good resource of battery (Long battery life)
- Durable metallic body
- Microprocessor controlled

<table>
<thead>
<tr>
<th>Frequency range</th>
<th>Antenna 1: 50-4000 MHz; Antenna 2: 2.44GHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>Two AAA batteries (2xLR03)</td>
</tr>
<tr>
<td>Dimensions</td>
<td>Without antennas: 120x70x16 mm</td>
</tr>
<tr>
<td></td>
<td>With antennas: 220x70x16 mm</td>
</tr>
<tr>
<td>Current consumption</td>
<td>Up to 30 mA</td>
</tr>
<tr>
<td>Operation duration</td>
<td>Up to 20 hours</td>
</tr>
<tr>
<td>Indications</td>
<td>Active antenna, Low battery, Mode, Identification, Attenuator, Secondary demodulation</td>
</tr>
</tbody>
</table>
The ‘IDENTIFICATION’ LED of the Protect 1206i changes color depending on the detected protocol:

- **BLUE** — BLUETOOTH
- **GREEN** — Wi-Fi
- **RED** — GSM900/1800
- **ORANGE** — DECT

**CITY antenna**

External sources of RF waves present in big cities such as cellular base stations, broadcasting antennas, industrial interference or any other sources of RF waves may cause full illumination of the Protect 1206’s bar graph in the ANT1 channel when the long, standard antenna is used; this may sometimes even happen with the attenuator. Obviously this complicates the sweeping procedure or can even make it impossible in certain cases.

The ‘CITY’ antenna allows the device to avoid interference from external sources in cities or near broadcasting towers etc. Therefore we suggest using the CITY antenna for the ANT1 channel as a replacement to the standard long antenna if you observe a high level on the bar graph of the Protect 1206i in most parts of the room.
The Protect 1206i has two separate RF channels which work with the two corresponding antennas. Number one (1) is 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. The second antenna, marked as 2.44GHz (2), is used for the detection of the other above mentioned protocols, such as Bluetooth, Wi-Fi, etc.

The usual method of searching suggests using the antenna marked as (1), i.e. 50-4000MHz, first in order to cover a wide range of frequencies. Then the procedure of scanning the area should be repeated with the second antenna (2) 2.44GHz selected.

Despite the second antenna (2) being tuned in the 2.44GHz range, it can also be used for identification of GSM900/1800 signals as it has narrower bandwidth, therefore all the interferences are ignored and the identification algorithm works more efficiently. This means the 2.44GHz antenna may be used temporarily during the first scan in order to study suspicious places in the room more precisely, or to identify digital transmissions if such signals appear. Use the ANT1 and ANT2 buttons (9) to select the corresponding antenna.

For assistance during the search the Protect 1206i has an active correlation mode. This function allows the operator to study the suspicious signals in certain cases. When the 'CORR' button (10) is pressed in close proximity to the suspicious area the unit produces probing 'beep' signals. The sound is picked up by a bug and then transmitted into the air. The unit will receive and demodulate transmitted waves and the operator can see signs of the probing signals on the DEMODULATION display (3). Fluctuations appearing simultaneously with the beeps will warn of an FM transmitter or other type of transmission which correlates with the sound.

The Protect 1206i has a 16-segment 'SIGNAL STRENGTH' bar graph indicator (6) providing precise information to the operator. The signals can be measured in the range of -30dB to +8dB. The closer the unit is to the source of transmission the higher bar graph level will be. Some powerful sources may cause full illumination of the display (or when the unit is in close proximity to the transmitter). In such cases use the attenuator function (ATT+/ATT- buttons (8) 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 for a search. Note that the vibration function will be turned on when the SIGNAL STRENGTH (6) approaches the 6th segment.

The MODE (4), control of the Protect 1206i is used for selecting the desired indication method. There are four modes available:

- 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
silent, when there is no sound and no vibration

The sound mode is convenient for a fast search as an experienced operator may be able to distinguish between different types of signals.

An FM-modulated transmitter (bug) can produce a 'loopback effect' when the unit is close to it, or cause the effect of a disappearance in background noises, which are usually present further away from the transmitter. In this case the 'hum' which can be heard in other parts of the room can disappear when the Protect 1206i approaches the transmitter and there will be silence from the unit's speaker. When this happens it is recommended to use the 'CORR' function (10) while watching the 'DEMODULATION' display (3). Simultaneous fluctuations will warn of danger. Please note that the sound mode is not suitable for covert searches, as the transmitter will 'hear' sounds in the room.

The vibration and mixed modes are convenient when probing difficult to reach objects and places. The operator can work without the necessity of watching the bar graph. a high RF level will be indicated by the vibration.

The Protect 1206i 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 (11) will turn on when the batteries are nearing exhaustion.

Usage

Sweeping the room

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

1. Leave the room, turn on your Protect 1206i (7) and select ANT1 (9). Watch the bar graph (6) and if it shows an increased level (more than 4-5 segments), turn on the attenuator by pressing the ATT+ button (8).
2. Choose the operation mode with the help of the MODE button (4).
   1) For covert procedures use the vibration mode or silent mode.
   2) The sound mode is more convenient for locating and inspecting the RF source.
3) The vibrating or mixed mode allows the operator to avoid constantly watching the bar graph when inspecting areas that are difficult to access. The sound mode allows the operator to listen to the signal so that he or she can understand more about the source. The FM-modulated transmitter (bug) can produce a 'loopback effect' when the unit is close to it or cause the effect of a disappearance of the background noises, which are usually present further away from the transmitter. In this case the 'hum' which can be heard in other parts of the room can disappear when the Protect 1206i approaches the transmitter and there is a silence on the speaker. In this case it is recommended to use the 'CORR' function (10) while watching the DEMODULATION' display (3). Simultaneous fluctuations will warn of the danger.

3. Enter the room holding the Protect 1206i while watching its bar graph 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 bugging device the bar graph of your Protect 1206i will rise (or the vibration will appear).

The distance of detection may vary depending on the situation. Usually the Protect 1206i is able to detect an average radio microphone at a distance of 20-80 cm, although it is recommended to probe objects at a proximity of 10 cm. The bar graph can display 16 different levels. You can use the attenuator to decrease the sensitivity when performing the location procedure (finding the source of the RF field). Press the ATT+ button 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 1206i by pressing the ATT- button.

The bar graph may often show an increased level near wires or metal objects. This may not be a bug, but rather the metal acting as an antenna extension. A similar situation may appear in the apertures of windows due to radio waves coming from the outside.

If you have found a suspicious area, switch the Protect 1206i to the second antenna 2.44GHz (2). In this mode the unit is much more sensitive to Bluetooth and Wi-Fi wireless protocols. It measures the level of the RF field which allows the operator to perform the location procedure. The 'IDENTIFICATION' LED (5) will show the corresponding color in accordance with the table printed on the front panel. After checking for the presence of wireless transmissions return the Protect 1206i to the initial state (ANT1) and continue searching.

4. Repeat the scanning procedure for the whole room with the ANT2 selected. Which will enable you to find sources of Bluetooth, Wi-Fi, GSM and some DECT transmissions. Please note: there are many variants of DECT sub-types so the
Protect 1206i may not recognize some of them with its IDENTIFICATION display. Nevertheless its 'SIGNAL STRENGTH' indicator will always show an increased level when approaching a source of DECT transmission. Try to train your hearing to recognize different types of wireless protocols:

- Bluetooth gives a 'crackle' sound
- Wi-Fi will produce a 'scratching' sound
- GSM gives a 'buzzing' (hum)
- DECT is heard as a 50Hz AC transformer hum

If you have found a source of wireless transmission inspect it very carefully. 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:

- Compact
- Hidden
- Handmade or produced with low quantity
- With 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 antenna
- With a SIM card inserted

5. After you have found the exact location of a high field, perform the following actions:

1) If secrecy is not critical turn on the sound mode and check for the presence of a loopback effect or the effect of a disappearance in background noise near the suspicious place
2) Press the CORR button while watching the DEMODULATION display to find the synchronous fluctuations. They will show the presence of correlation, i.e. a radio microphone.
3) Select ANT2 and check for the presence of wireless protocols as described above

Not depending on the results, start 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. Remember, that a physical search is a fundamental operation during the 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

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. Place the Protect 1206i 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 it 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**

There are many types of body-carried transmitters. They may broadcast conversations and (or) video signals. Turn on the attenuator if necessary. While carrying the Protect 1206i, approach the person. If the bar graph level grows, it means that the person is carrying 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 1206i on the desktop. In this case, it is necessary to watch the bar graph carefully when the person approaches the table and sits down.

**Other applications**

If you cannot inspect a whole room, for example, in a restaurant or someone else's office, the Protect 1206i 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 1206i depends on two major factors:

- The output power of the transmitter
- The surrounding RF environment, such as radio/TV and communication devices

The level on the display of the Protect 1206i 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 1206i. Normally, an active FM-transmitter will be detected at a distance of 20-80 cm; GSM transmitter at 50-150 cm; Bluetooth transmitter at 10-50 cm; Wi-Fi transmitter at 10-100 cm.