RadioInspectorWiFi is a new sight on the wireless network analysis

Before we start, just a little bit of statistics.

Throughout one trip from one side of the city to another with switched RadioInspector Wi-Fi module on, we detected 4 034 unique MAC addresses including 1018 hotspots and 2 352 devices in the idle mode. In the most common cases, there were mobile phones whose owners did not switch off a Wi-Fi mode. We also detected 82 hidden networks that do not transmit SSIDs and work in point-to-point mode.

It's hard to find any other RF range so busy as a 2,4 GHz range. There are a lot of various signals on air: Bluetooth, ZigBee, analogue and digital cameras, remote access systems, microwave stoves etc. The more busy frequency range the more difficult to administrate and analyze it. This circumstance is the most common reason why intruders use this frequency range to conceal their illicit transmitters.

It is a very logical decision to use the same standards that are used within frequency range of interest for the illicit transmitters to maximize their concealment effectiveness. The Wi-Fi is one of the most reasonable standards that can be used to provide such kind transmission due to low cost and affordable components and sustainable engineering decisions. However, first of all, it is hard to discern two digital devices that use the same standard without extracting their unique IDs, when one of them is a legal device and other one is a clandestine transmitter. In case of the Wi-Fi the key facet is MAC address of the device.

We will not consider questions of Internet and Intranet security, these questions are beyond of theme of this article. In our case, we consider the Wi-Fi as a channel of information leakage and what requirements can be implemented to the contemporary Wi-Fi monitoring systems.

An interesting description of a Wi-Fi voice recorder were presented in 2013 on the web site of the English company WINKELMANN . At the first time this device were presented under name "WREN WiFi" and then "ACU-GEM WiFi" but on the web site of the Irish company "ACUSTEK LTD".

Here you can see some key aspects of the description of this device derived from the web site "Gedion LTD" where this recorder already has name "KATANA FT-1":

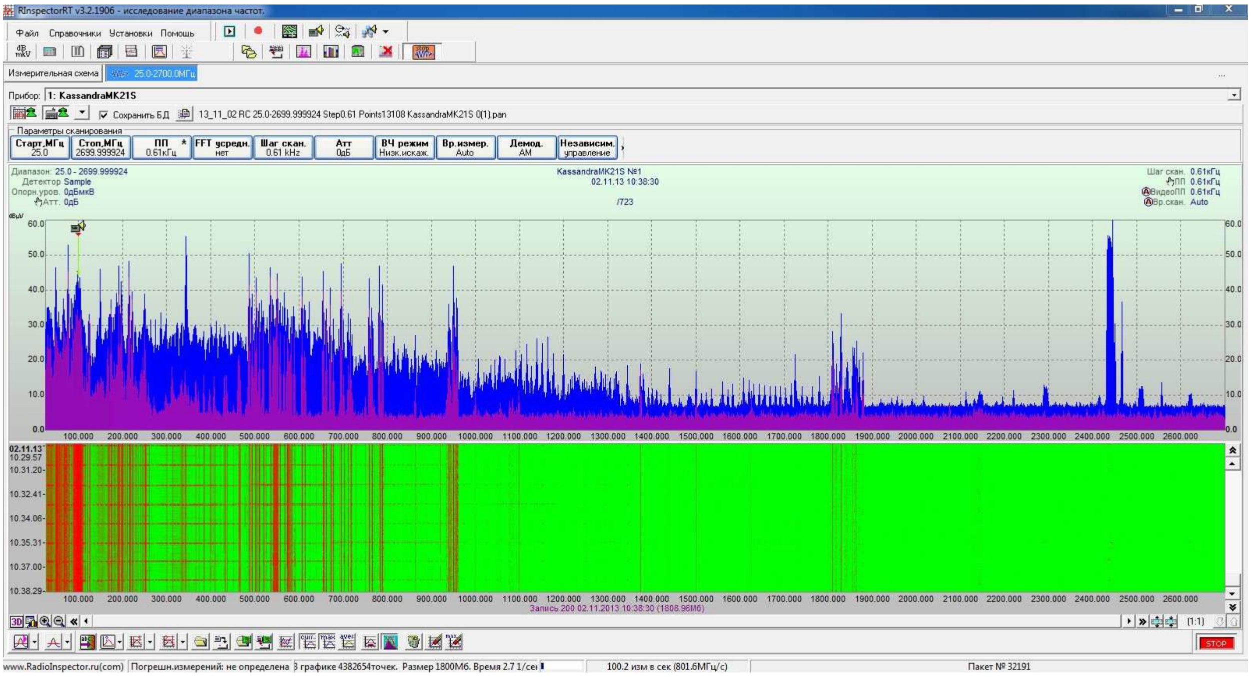
"The high quality mini voice recorder with a built-in Wi-Fi transmitter.

Wi-Fi voice recorder "Katana FT-1" is a unique device that combines advantages and devoid of disadvantages of voice recorders and transmitters. In contradistinction to various standard voice recorders, the wireless Wi-Fi recorder "Katana FT-1" does not need a direct access to it. The concealed voice recorder is able to derive and transfer information throughout many years. ***In contradistinction to standard RF transmitters, the Wi-Fi voice recorder needs just some minutes of transmission time a day to transfer all recorded data to a recipient, that is why this recorder is hard to detect by EMF detector or by TSCM system.*** *The size of the recorder is less than two jointed lighters. The recorder supports various changeable microSD cards. The supported volume of memory allows storage up to 300 hours of voice information with the sample rate 8kHz. The built-in battery provides up to 120 hours of autonomous work (without an external power supply).* ***Uploading of 24 hours of surveillance requires just some minutes.***

The kit contains a mini router Wi-Fi, which can be connected to a PC. The Wi-Fi voice recorder supports a configuration, which allows it to detect a mini-router's network and then connect to it and transfer the retained data.

“Katana FT-1” also can be configured to work within an established Wi-Fi network – in an office Intranet, for instance. In this case, the recorder can transfer a gained information to a remote PC in according to schedule.”

Nowadays voice recorders like a described above can be bought in many various internet shops around the world. A little bit of cunning, of course, is present in the description of the Wi-Fi recorder – every device, which transmits information might be detected. However, detection of this device during recording is obviously a challenge, because of its spurious emission is hard to differentiate with many other signals on the background. The figure 2 shows a spurious emission of the particular Wi-Fi voice recorder, which was detected with very sensitive and sophisticated equipment the distance was just a few centimeters. That is why detection of this device is much more effective during its transmission session via Wi-Fi network.


RInspectorRT v3.2.1906 - исследование диапазона частот.

Прибор: 1: KassandraMK21S

☑ Сохранить БД 13_11_02 RC 25.0-2699.999924 Step0.61 Points13108 KassandraMK21S 0(1).pan

Параметры сканирования

Старт,МГц	Стоп,МГц	ПП *	FFT усредн.	Шаг скан.	Атт	ВЧ режим	Вр.измер.	Демод.	Независим.
25.0	2699.999924	0.61кГц	нет	0.61 kHz	0дБ	Низк.искаж.	Auto	AM	управление

Диапазон: 25.0 - 2699.999924
Детектор Sample
Опорн.уров. 0дБмкВ
Атт. 0дБ

KassandraMK21S №1
02.11.13 10:38:30
/723

Шаг скан. 0.61кГц
ПП 0.61кГц
ВидеоПП 0.61кГц
Вр.скан. Auto

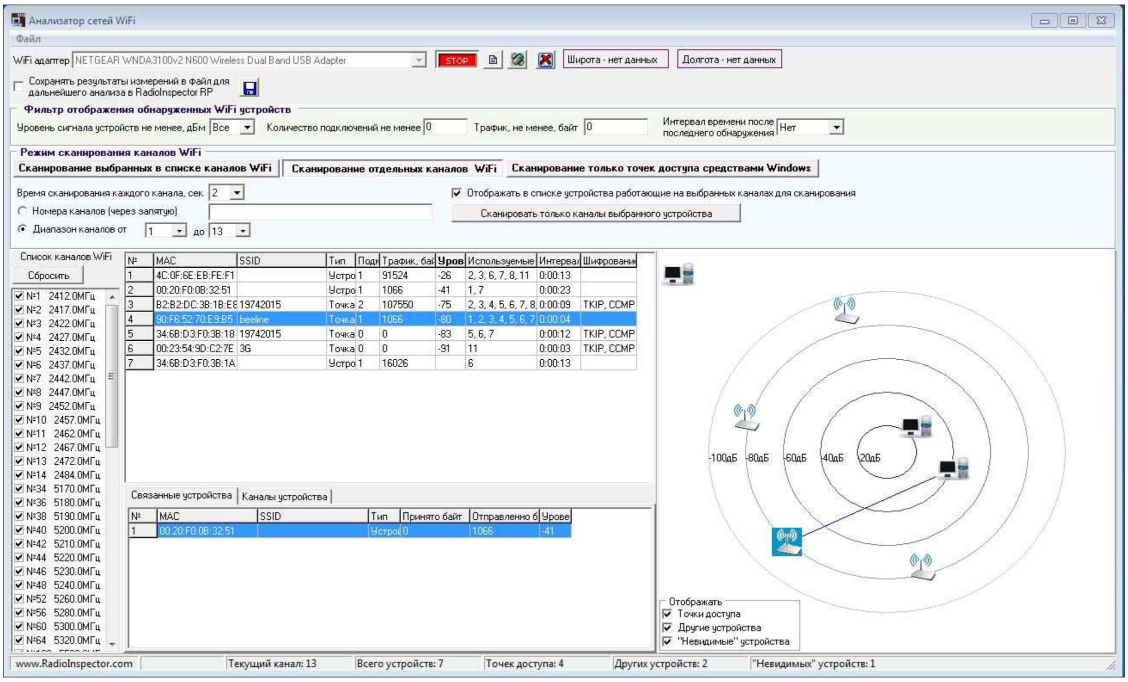
Запись 200 02.11.2013 10:38:30 (1808.96Мб)

www.RadioInspector.ru(com) | Погрешн.измерений: не определена | В графике 4382654точек. Размер 1800Мб. Время 2.7 1/се | 100.2 изм в сек (801.6МГц/с) | Пакет № 32191

Figure 2. The spurious emission of the Wi-Fi voice recorder

We conducted our own tests and confirm all of announced parameters of this voice recorder. We want to emphasize the following features:

The voice recorder can be detected as a Wi-Fi hotspot with any kind of name. In our case a very popular mobile operator’s name was chosen for the SSID name (Figure 3.).



Анализатор сетей WiFi

Файл

WiFi адаптер: NETGEAR WNDA3100v2 N600 Wireless Dual Band USB Adapter

Широта - нет данных

Долгота - нет данных

□ Сохранять результаты измерений в файл для дальнейшего анализа в RadioInspector RP

Фильтр отображения обнаруженных WiFi устройств

Уровень сигнала устройств не менее, дБм: Все

Количество подключений не менее: 0

Трафик, не менее, байт: 0

Интервал времени после последнего обнаружения: Нет

Режим сканирования каналов WiFi

Сканирование выбранных в списке каналов WiFi | Сканирование отдельных каналов WiFi | Сканирование только точек доступа средствами Windows

Время сканирования каждого канала, сек: 2

○ Номера каналов (через запятую)

● Диапазон каналов от 1 до 13

☑ Отображать в списке устройства работающие на выбранных каналах для сканирования

Сканировать только каналы выбранного устройства

Список каналов WiFi

Сбросить

☑ №1 2412.0МГц
☑ №2 2417.0МГц
☑ №3 2422.0МГц
☑ №4 2427.0МГц
☑ №5 2432.0МГц
☑ №6 2437.0МГц
☑ №7 2442.0МГц
☑ №8 2447.0МГц
☑ №9 2452.0МГц
☑ №10 2457.0МГц
☑ №11 2462.0МГц
☑ №12 2467.0МГц
☑ №13 2472.0МГц
☑ №14 2484.0МГц
☑ №34 5170.0МГц
☑ №36 5180.0МГц
☑ №38 5190.0МГц
☑ №40 5200.0МГц
☑ №42 5210.0МГц
☑ №44 5220.0МГц
☑ №46 5230.0МГц
☑ №48 5240.0МГц
☑ №52 5260.0МГц
☑ №56 5280.0МГц
☑ №60 5300.0МГц
☑ №64 5320.0МГц

№	MAC	SSID	Тип	Подк	Трафик, бай	Уров	Используемые	Интервал	Шифровани
1	4C:0F:6E:EB:FE:F1		Устро	1	91524	-26	2, 3, 6, 7, 8, 11	0:00:13	
2	00:20:F0:0B:32:51		Устро	1	1066	-41	1, 7	0:00:23	
3	B2:B2:DC:3B:1B:E8	19742015	Точка	2	107550	-75	2, 3, 4, 5, 6, 7, 8,	0:00:09	TKIP, CCMP
4	90:F6:52:70:E9:B5	beeline	Точка	1	1066	-80	1, 2, 3, 4, 5, 6, 7	0:00:04	
5	34:6B:D3:F0:3B:18	19742015	Точка	0	0	-83	5, 6, 7	0:00:12	TKIP, CCMP
6	00:23:54:9D:C2:7E	3G	Точка	0	0	-91	11	0:00:03	TKIP, CCMP
7	34:6B:D3:F0:3B:1A		Устро	1	16026		6	0:00:13	

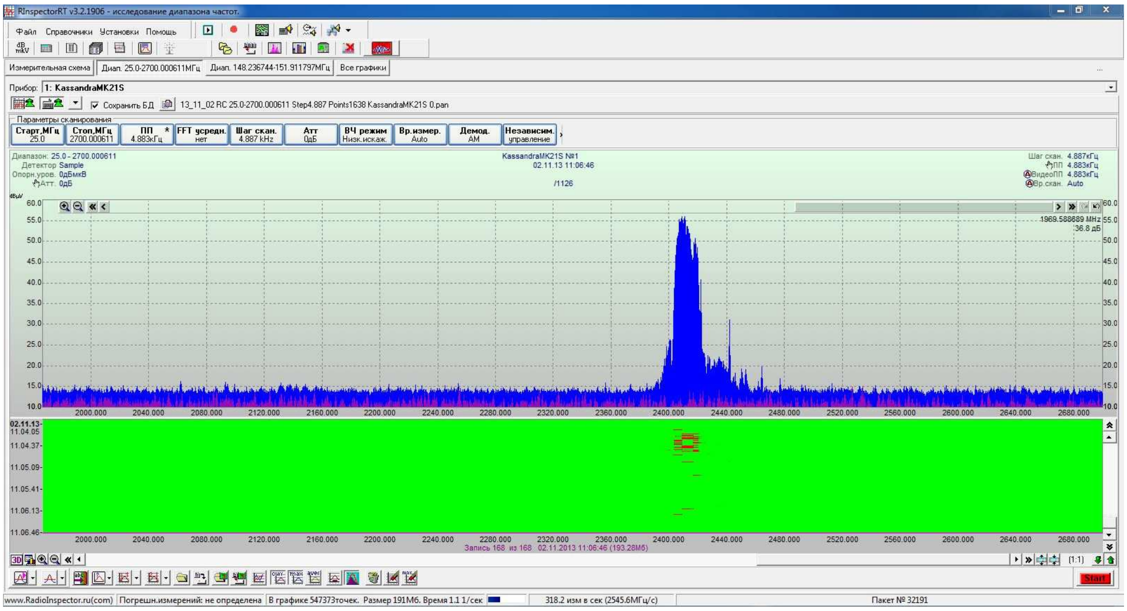
Связанные устройства | Каналы устройства

№	MAC	SSID	Тип	Принято байт	Отправленно б	Урове
1	00:20:F0:0B:32:51		Устрої	0	1066	-41

Отображать
☑ Точки доступа
☑ Другие устройства
☑ "Невидимые" устройства

www.RadioInspector.com | Текущий канал: 13 | Всего устройств: 7 | Точек доступа: 4 | Других устройств: 2 | "Невидимых" устройств: 1

1. The transmission of the 30 minutes of conversation took us 30 seconds (Figure 4).



RInspectorRT v3.2.1906 - исследование диапазона частот.

Измерительная схема | Диап. 25.0-2700.000611МГц | Диап. 148.236744-151.911797МГц | Все графики

Прибор: 1: KassandraMK21S

☑ Сохранить БД 13_11_02 RC 25.0-2700.000611 Step4.887 Points1638 KassandraMK21S 0.pan

Параметры сканирования

Старт,МГц	Стоп,МГц	ПП *	FFT усредн.	Шаг скан.	Атт	ВЧ режим	Вр.измер.	Демод.	Независим.
25.0	2700.000611	4.883кГц	нет	4.887 kHz	0дБ	Низк.искаж.	Auto	AM	управление

Диапазон: 25.0 - 2700.000611
Детектор Sample
Опорн.уров. 0дБмкВ
Атт. 0дБ

KassandraMK21S №1
02.11.13 11:06:46
/1126

Шаг скан. 4.887кГц
ПП 4.883кГц
ВидеоПП 4.883кГц
Вр.скан. Auto

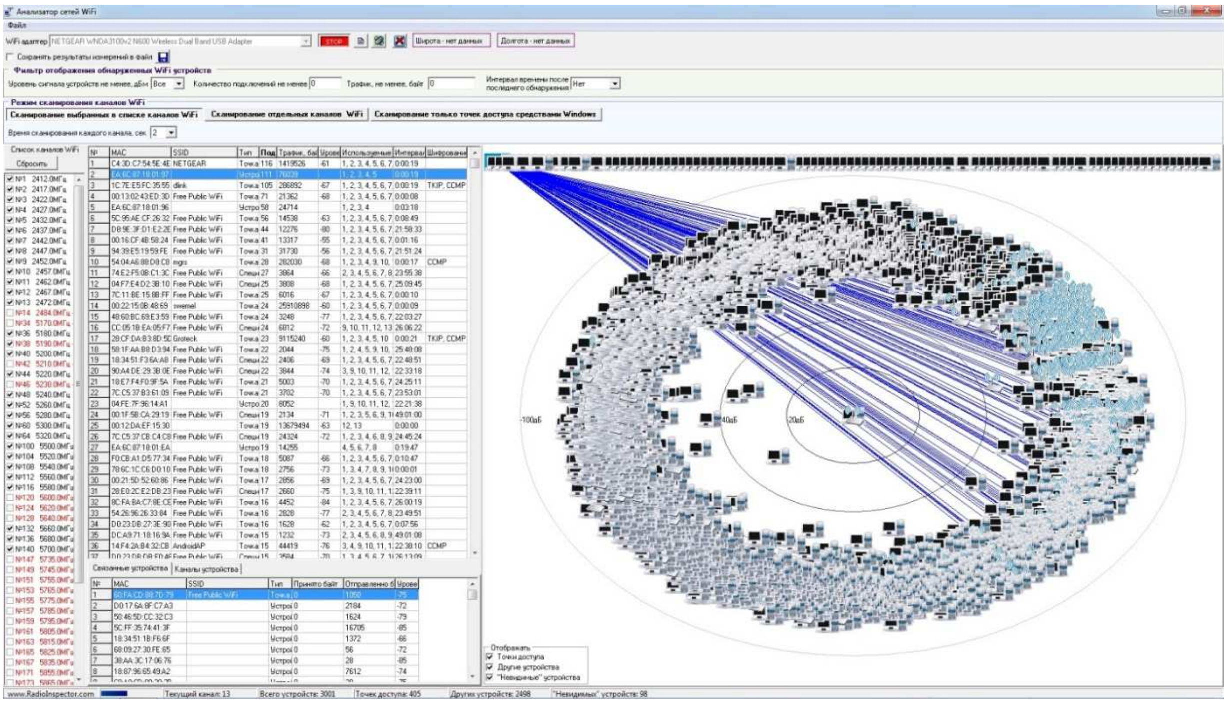
1969.588689 MHz
36.8 дБ

Запись 168 из 168 02.11.2013 11:06:46 (193.28Мб)

www.RadioInspector.ru(com) | Погрешн.измерений: не определена | В графике 547373точек. Размер 191Мб. Время 1.1 1/сек | 318.2 изм в сек (2545.6МГц/с) | Пакет № 32191

It was a very first signal for the reassessment of the approach of monitoring of the Wi-Fi networks. **An uninterruptible and permanent monitoring of the Wi-Fi network is actual and must be present in any organization, which is interested in controlling of the information leakage channels.**

Let’s consider an environment around a premise inside a business center with many Wi-Fi hotspots and a large amount of different mobile devices connected to them. In such kind circumstances it is hard to detect a new hotspot with a name very similar to the already present. For instance, SSID "Orange Wi-Fi" vs "OrangeWi-Fi". It is crucial to know MAC addresses all of legal devices in your premise and provide an automatic monitoring any changes within the Wi-Fi environment.



Анализатор сетей WiFi

Файл

WiFi адаптер: NETGEAR WNDA3100v2 N600 Wireless Dual Band USB Adapter

☐ Сохранять результаты измерений в файл

Широта - нет данных | Долгота - нет данных

Фильтр отображения обнаруженных WiFi устройств

Уровень сигнала устройств не менее, дБм: Все | Количество подключений не менее: 0 | Трафик, не менее, байт: 0 | Интервал времени после последнего обнаружения: Нет

Режим сканирования каналов WiFi

Сканирование выбранных в списке каналов WiFi | Сканирование отдельных каналов WiFi | Сканирование только точек доступа средствами Windows

Время сканирования каждого канала, сек: 2

Список каналов WiFi

☑ №1 2412.0МГц
☑ №2 2417.0МГц
☑ №3 2422.0МГц
☑ №4 2427.0МГц
☑ №5 2432.0МГц
☑ №6 2437.0МГц
☑ №7 2442.0МГц
☑ №8 2447.0МГц
☑ №9 2452.0МГц
☑ №10 2457.0МГц
☑ №11 2462.0МГц
☑ №12 2467.0МГц
☑ №13 2472.0МГц
☐ №14 2484.0МГц
☐ №34 5170.0МГц
☑ №36 5180.0МГц
☑ №38 5190.0МГц
☑ №40 5200.0МГц
☐ №42 5210.0МГц
☑ №44 5220.0МГц
☐ №46 5230.0МГц
☑ №48 5240.0МГц
☑ №52 5260.0МГц
☑ №56 5280.0МГц
☑ №60 5300.0МГц
☑ №64 5320.0МГц
☑ №100 5500.0МГц
☑ №104 5520.0МГц
☑ №108 5540.0МГц
☑ №112 5560.0МГц
☑ №116 5580.0МГц
☐ №120 5600.0МГц
☐ №124 5620.0МГц
☐ №128 5640.0МГц
☑ №132 5660.0МГц
☑ №136 5680.0МГц
☑ №140 5700.0МГц
☐ №147 5735.0МГц
☐ №149 5745.0МГц
☐ №151 5755.0МГц
☐ №153 5765.0МГц
☐ №155 5775.0МГц
☐ №157 5785.0МГц
☐ №159 5795.0МГц
☐ №161 5805.0МГц
☐ №163 5815.0МГц
☐ №165 5825.0МГц
☐ №167 5835.0МГц
☐ №171 5855.0МГц

№	MAC	SSID	Тип	Под	Трафик, бай	Уровен	Используемые	Интервал	Шифрование
1	C4:3D:C7:54:5E:4E	NETGEAR	Точка	116	1419526	-61	1, 2, 3, 4, 5, 6, 7,	0:00:19	
2	EA:6C:87:18:01:97		Устро	111	76029		1, 2, 3, 4, 5	0:00:19	
3	1C:7E:E5:FC:35:55	dlink	Точка	105	286892	-67	1, 2, 3, 4, 5, 6, 7,	0:00:19	TKIP, CCMP
4	00:13:02:43:ED:3D	Free Public WiFi	Точка	71	21362	-68	1, 2, 3, 4, 5, 6, 7,	0:00:08	
5	EA:6C:87:18:01:96		Устро	58	24714		1, 2, 3, 4	0:03:18	
6	5C:95:AE:CF:26:32	Free Public WiFi	Точка	56	14538	-63	1, 2, 3, 4, 5, 6, 7,	0:08:49	
7	D8:9E:3F:D1:E2:2E	Free Public WiFi	Точка	44	12276	-80	1, 2, 3, 4, 5, 6, 7,	21:58:33	
8	00:16:CF:48:58:24	Free Public WiFi	Точка	41	13317	-55	1, 2, 3, 4, 5, 6, 7,	0:01:16	
9	94:39:E5:19:59:FE	Free Public WiFi	Точка	31	31730	-56	1, 2, 3, 4, 5, 6, 7,	21:51:24	
10	54:04:A6:88:D8:C8	mgts	Точка	28	282030	-68	1, 2, 3, 4, 9, 10,	0:00:17	CCMP
11	74:E2:F5:08:C1:3C	Free Public WiFi	Специ	27	3864	-66	2, 3, 4, 5, 6, 7, 8,	23:55:38	
12	04:F7:E4:D2:38:10	Free Public WiFi	Специ	25	3808	-68	1, 2, 3, 4, 5, 6, 7,	25:09:45	
13	7C:11:BE:15:88:FF	Free Public WiFi	Точка	25	6016	-67	1, 2, 3, 4, 5, 6, 7,	0:00:10	
14	00:22:15:08:48:69	sveme!	Точка	24	25910898	-60	1, 2, 3, 4, 5, 6, 7	0:00:09	
15	48:60:BC:69:E3:59	Free Public WiFi	Точка	24	3248	-77	1, 2, 3, 4, 5, 6, 7,	22:03:27	
16	CC:05:18:EA:05:F7	Free Public WiFi	Специ	24	6812	-72	9, 10, 11, 12, 13	26:06:22	
17	28:CF:DA:B3:8D:5C	Groteck	Точка	23	9115240	-60	1, 2, 3, 4, 5, 10	0:00:21	TKIP, CCMP
18	58:1F:AA:B8:D3:94	Free Public WiFi	Точка	22	2044	-75	1, 2, 4, 5, 9, 10,	25:40:08	
19	18:34:51:F3:6A:A8	Free Public WiFi	Специ	22	2406	-69	1, 2, 3, 4, 5, 6, 7,	22:48:51	
20	90:A4:DE:29:3B:0E	Free Public WiFi	Специ	22	3844	-74	3, 9, 10, 11, 12,	22:33:18	
21	18:E7:F4:F0:9F:5A	Free Public WiFi	Точка	21	5003	-70	1, 2, 3, 4, 5, 6, 7,	24:25:11	
22	7C:C5:37:B3:61:09	Free Public WiFi	Точка	21	3702	-70	1, 2, 3, 4, 5, 6, 7,	23:53:01	
23	04:FE:7F:96:14:A1		Устро	20	8052		1, 9, 10, 11, 12,	22:21:38	
24	00:1F:5B:CA:29:19	Free Public WiFi	Специ	19	2134	-71	1, 2, 3, 5, 6, 9, 1	49:01:00	
25	00:12:DA:EF:15:30		Точка	19	13679494	-63	12, 13	0:00:00	
26	7C:C5:37:C8:C4:C8	Free Public WiFi	Специ	19	24324	-72	1, 2, 3, 4, 6, 8, 9,	24:45:24	
27	EA:6C:87:18:01:EA		Устро	19	14255		4, 5, 6, 7, 8	0:19:47	
28	F0:CB:A1:D5:77:34	Free Public WiFi	Точка	18	5087	-66	1, 2, 3, 4, 5, 6, 7,	0:10:47	
29	78:6C:1C:C6:D0:10	Free Public WiFi	Точка	18	2756	-73	1, 3, 4, 7, 8, 9, 1	0:00:01	
30	00:21:5D:52:60:86	Free Public WiFi	Точка	17	2856	-69	1, 2, 3, 4, 5, 6, 7,	24:23:00	
31	28:E0:2C:E2:DB:23	Free Public WiFi	Специ	17	2660	-75	1, 3, 9, 10, 11, 1	22:39:11	
32	8C:FA:BA:C7:8E:CE	Free Public WiFi	Точка	16	4452	-84	1, 2, 3, 4, 5, 6, 7,	26:00:19	
33	54:26:96:26:33:84	Free Public WiFi	Точка	16	2828	-77	2, 3, 4, 5, 6, 7, 8,	23:49:51	
34	D0:23:DB:27:3E:90	Free Public WiFi	Точка	16	1628	-62	1, 2, 3, 4, 5, 6, 7,	0:07:56	
35	DC:A9:71:18:16:9A	Free Public WiFi	Точка	15	1232	-73	2, 3, 4, 5, 6, 8, 9,	49:01:08	
36	14:F4:2A:84:32:CB	AndroidAP	Точка	15	44419	-76	3, 4, 9, 10, 11, 1	22:38:10	CCMP

Связанные устройства | Каналы устройства

№	MAC	SSID	Тип	Принято байт	Отправленно б	Уровен
1	60:FA:CD:88:7D:79	Free Public WiFi	Точка	0	1050	-75
2	D0:17:6A:8F:C7:A3		Устрой	0	2184	-72
3	50:46:5D:CC:32:C3		Устрой	0	1624	-79
4	5C:FF:35:74:41:3F		Устрой	0	16705	-85
5	18:34:51:1B:F6:6F		Устрой	0	1372	-66
6	68:09:27:30:FE:65		Устрой	0	56	-72
7	38:AA:3C:17:06:76		Устрой	0	28	-85
8	18:87:96:65:49:A2		Устрой	0	7612	-74

Отображать
☑ Точки доступа
☑ Другие устройства
☑ "Невидимые" устройства

www.RadioInspector.com | Текущий канал: 13 | Всего устройств: 3001 | Точек доступа: 405 | Других устройств: 2498 | "Невидимых" устройств: 98

Figure 5. Hundreds of Wi-Fi devices around the controlled premise

No doubt, the threat of interception of information by means of Wi-Fi devices is real. However, we should take into account that voice recorder with the price about $2500 can buy not every curious person.

Another one feature that uses advantages of Wi-Fi is a wireless video camera. Let’s consider a very popular and affordable model Defender MULTICAM WF-10HD. It’s pretty enough to get acquainted with the description of this device to understand it can be very useful tool for the surveillance. The camera is accessible via especial Internet resource. The main problem is to switch the camera on via Internet. After the activation, you will see the same picture as was described above - a new Wi-Fi hotspot. Meanwhile, this device can also store video onto the built-in SD card and then transfer information in a convenient moment.

What is the most common problem with contemporary Wi-Fi network analyzers that used by security staff? These analyzers are connected directly to the controlling PC that usually placed in a special room far enough from controlled premise. This situation just increases the threat, because an illicit transmitter might be missed.

The requirements to a Wi-Fi monitoring system

The following requirements to a Wi-Fi monitoring system are based on a huge run experience of the TSCM work and analysis of channels of information leakage:

1. Uninterruptible 7/24 monitoring of the whole Wi-Fi range standards (IEEE 802.11 a/b/g/n), with the time-bound.
2. An ability to install a monitoring unit in a controlled area directly without a management PC.
3. An ability of work in an autonomous mode without a direct connection to the controlling PC for information storage.

4. Maintaining of the list of MAC addresses of detected devices for the fast detection and identification.
5. Multi domain distributed network of monitoring devices support.
6. A lightweight, compact and economy receiving module for operational tasks of detection and analysis of the wireless network.

On the base of described above requirements, a new generation of the soft&hardware system RadioInspectorWiFi with the receiver RSWIFI was developed.

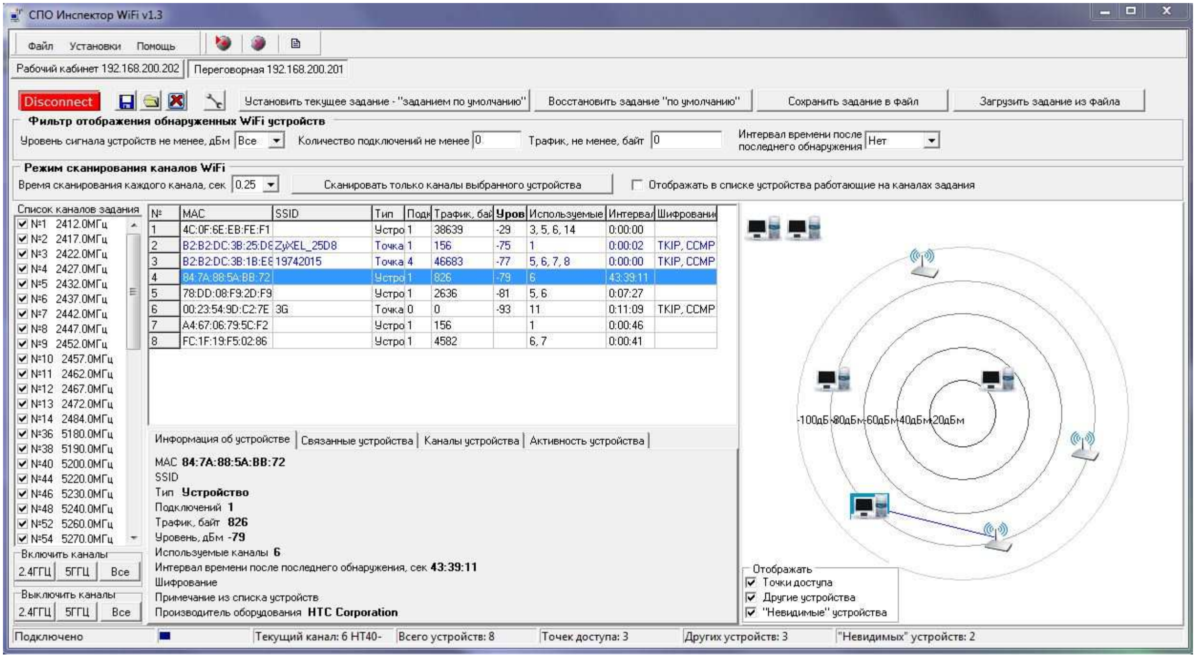
Figure 6. RadioInspector WiFi

What kind changes were made?

First of all, a new receiver, which is able to intercept all modern Wi-Fi standards IEEE 802.11 a/b/g/n was developed. The receiver contains its own microcomputer that can work in autonomous mode without connection to a PC. The memory of the microcomputer is calculated to retain automatically collected data throughout up to one year. The microcomputer has a nonvolatile memory. The OS loads and process of network monitoring starts immediately after the power is switched on.

The software now supports not only single server connection, but distributed monitoring network as well. A vast amount of monitoring systems can be connected to a controlling PC. The monitoring module connects to a controlling PC via 100Base-T interface. It is possible to build a monitoring network by installing modules within building that should be under control. Eventually, any attempt to bring a Wi-Fi device to a controlled premise and switch it on will be detected. The receiving module might be connected to a tablet PC, in this case it becomes a mobile system not for detection only, but localization by relative signal’s strength.

The frontend of the RadioInspectorWIFI is similar to the first program's generation, but has some important add-ons (See figure 7). The opportunity to upload a retained archive to a receiver is added. User also can get information about a producer of the Wi-Fi module based on the MAC address analysis. It is important to emphasize, the instrument has no restrictions concerned to quantity of channels being under control. All channels within two specified frequency ranges are under control.



Фильтр отображения обнаруженных WiFi устройств

Уровень сигнала устройств не менее, дБм: Все

Количество подключений не менее: 0

Трафик, не менее, байт: 0

Интервал времени после последнего обнаружения: Нет

Режим сканирования каналов WiFi

Время сканирования каждого канала, сек: 0.25

□ Отображать в списке устройства работающие на каналах задания

Список каналов задания

☑ №1 2412.0МГц
☑ №2 2417.0МГц
☑ №3 2422.0МГц
☑ №4 2427.0МГц
☑ №5 2432.0МГц
☑ №6 2437.0МГц
☑ №7 2442.0МГц
☑ №8 2447.0МГц
☑ №9 2452.0МГц
☑ №10 2457.0МГц
☑ №11 2462.0МГц
☑ №12 2467.0МГц
☑ №13 2472.0МГц
☑ №14 2484.0МГц
☑ №36 5180.0МГц
☑ №38 5190.0МГц
☑ №40 5200.0МГц
☑ №44 5220.0МГц
☑ №46 5230.0МГц
☑ №48 5240.0МГц
☑ №52 5260.0МГц
☑ №54 5270.0МГц

№	MAC	SSID	Тип	Подк	Трафик, бай	Уров	Используемые	Интервал	Шифровани
1	4C:0F:6E:EB:FE:F1		Устро	1	38639	-29	3, 5, 6, 14	0:00:00	
2	B2:B2:DC:3B:25:D8	ZyXEL_25D8	Точка	1	156	-75	1	0:00:02	TKIP, CCMP
3	B2:B2:DC:3B:1B:E8	19742015	Точка	4	46683	-77	5, 6, 7, 8	0:00:00	TKIP, CCMP
4	84:7A:88:5A:BB:72		Устро	1	826	-79	6	43:39:11	
5	78:DD:08:F9:2D:F9		Устро	1	2636	-81	5, 6	0:07:27	
6	00:23:54:9D:C2:7E	3G	Точка	0	0	-93	11	0:11:09	TKIP, CCMP
7	A4:67:06:79:5C:F2		Устро	1	156		1	0:00:46	
8	FC:1F:19:F5:02:86		Устро	1	4582		6, 7	0:00:41	

MAC **84:7A:88:5A:BB:72**
SSID
Тип **Устройство**
Подключений **1**
Трафик, байт **826**
Уровень, дБм **-79**
Используемые каналы **6**
Интервал времени после последнего обнаружения, сек **43:39:11**
Шифрование
Примечание из списка устройств
Производитель оборудования **HTC Corporation**

Отображать
☑ Точки доступа
☑ Другие устройства
☑ "Невидимые" устройства

Подключено | Текущий канал: 6 HT40- | Всего устройств: 8 | Точек доступа: 3 | Других устройств: 3 | "Невидимых" устройств: 2

Figure 7. The program interface.

Sometimes it is hard to organize an update of the device like a remote monitoring system. Our new RSWIFI module supports a remote firmware update via local network.

Such kind approach to building of the wireless network monitoring system seems to us a very perspective from the point of the detection of illicit network access and monitoring of information leakage channels.

What is the next?

The receiver is already able to support a GPS receiver. This extension allows not only collect and store collected MACs, but store GPS coordinates where this MAC has been detected. Highly likely, a geo option will be added to the next version of the RadioInspectorWiFi. The software with GPS option enabled can be used for mobile Wi-Fi analysis based on a car, including an autonomous analysis. It is enough to connect the receiver to a powerbank with 5V output (Figure 8), and system starts Wi-Fi network analysis with geospatial coordinates included.

Icom company has announced their new mobile stations that use a Wi-Fi network to communicate to each other. These mobile stations are intended to unite radio communications and IP technologies. This feature allows communicate various mobile stations that can't reach each other with a radio signal.

Another one important thing that worth to be mentioned is a new Bluetooth 4.0 feature. This feature was detected coincidently during the testing Bluetooth transmission by our new hardware system. We couldn't detect a data transmission between two modern devices with Bluetooth 4.0 transmitters. We only could intercept the beginning of transmission and then the signal had disappeared, but the devices indicated that transmission is still going well, the same time the counter of Bluetooth packets has stopped. The sophisticated analysis of the spectrum with RadioInspectorWiFi allowed us to detect a new network with SSID, which name consists a real name of the device that involved in transmission process. What does it mean? It means if any device that supports Bluetooth 4.0 has a Wi-Fi transmitter and a file being transmitted is big enough, in this case this device will try to establish connection via Wi-Fi by organizing a new wireless network between transmitter and recipient. What is the threat? A Wi-Fi transmission is more powerful than Bluetooth and can be easily intercepted by third party and name of the device allows intruders to understand, who is a real owner of the device with this MAC address. No one of the owners of the confidential information will be glad to know this. Of course, manufacturers should inform customers about this feature, but they don’t.