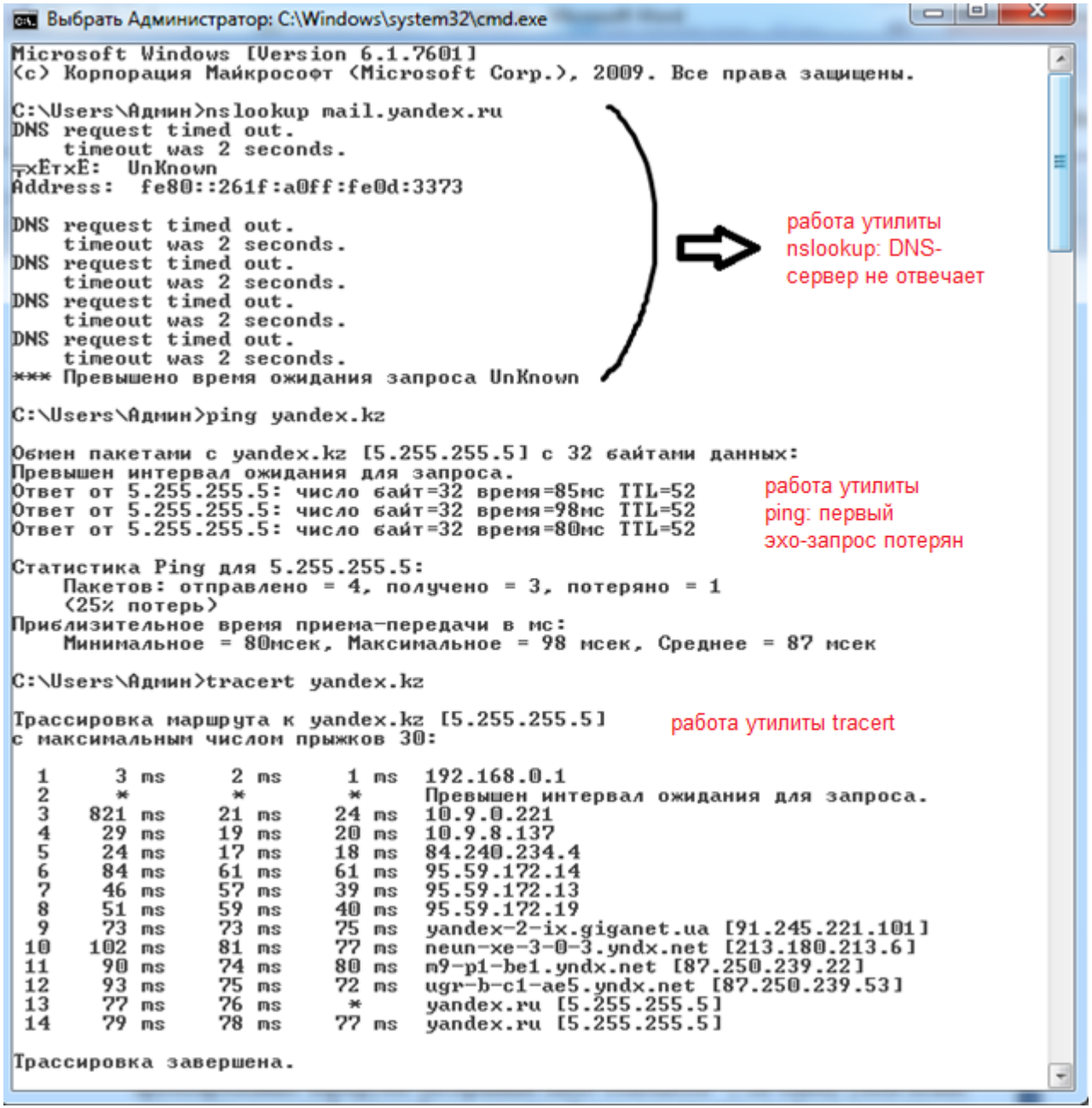
Программные средства анализа беспроводных сетей радиодоступа

Практики 1

Специализированные утилиты мониторинга

- Утилита **nslookup** предназначена для формирования запросов к серверам DNS из командной строки. Она является аналогом службы DNS-клиент и позволяет диагностировать проблемы с разрешением имен в системе DNS. По умолчанию все запросы отправляются на DNS-сервер, адрес которого задан настройками сетевого подключения. В терминах утилиты такой сервер является сервером по умолчанию (default server). Утилита nslookup позволяет определить как адреса IPv4, так и IPv6.
- Утилита **ping** формирует эхо-запросы и эхо-ответы с использованием пакетов протокола ICMP. Принцип работы утилиты подразумевает получение ответа только от конечного узла.
- Утилита **tracert** (tceroute для решений на Linux) обычно используется совместно с утилитой ping и позволяет уточнить проблемы на сети. Для формирования запросов и ответов также используется протокол ICMP, но для определения доступности промежуточных узлов используется манипулирование значением TTL.



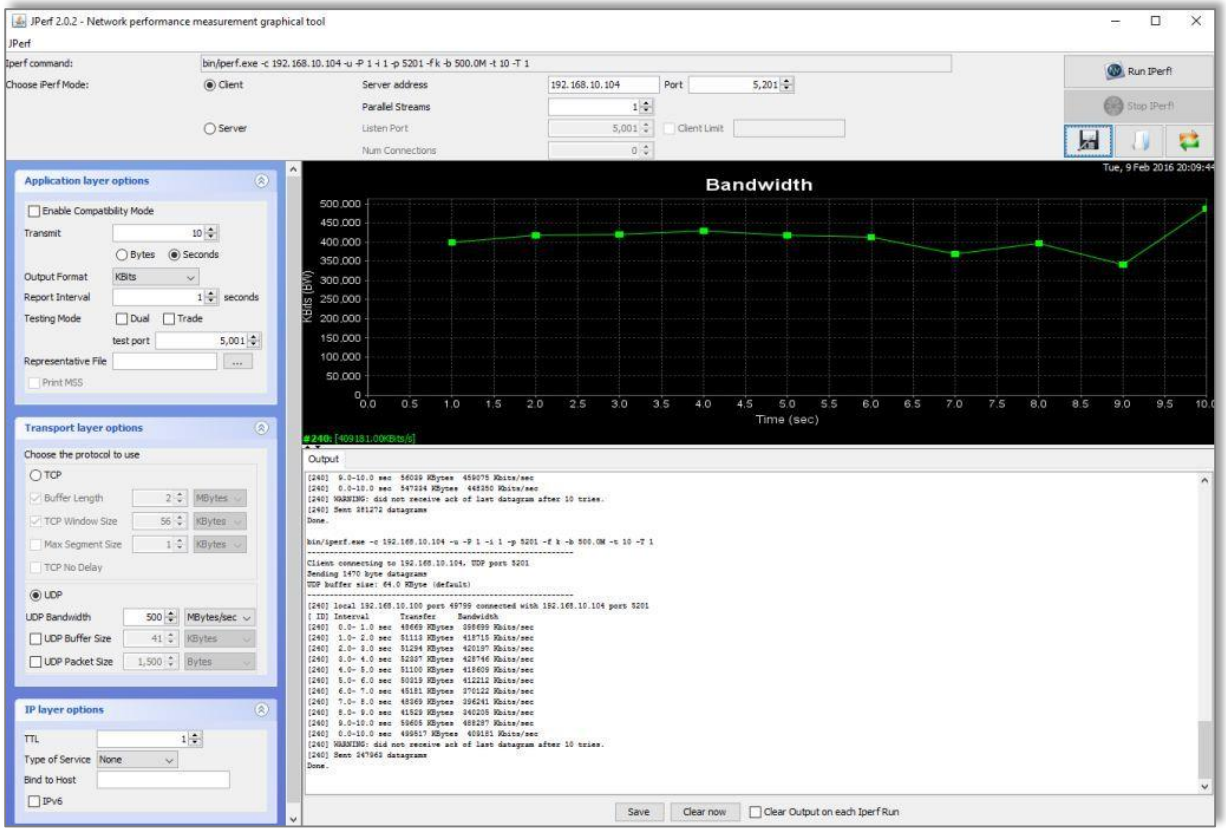
Утилиты используют IP-сеть, поэтому применяются только в случае реализации сетевой среды TCP/IP.

Не подходят для анализа физических свойств радиоканала, но отражают доступность сетевой среды.

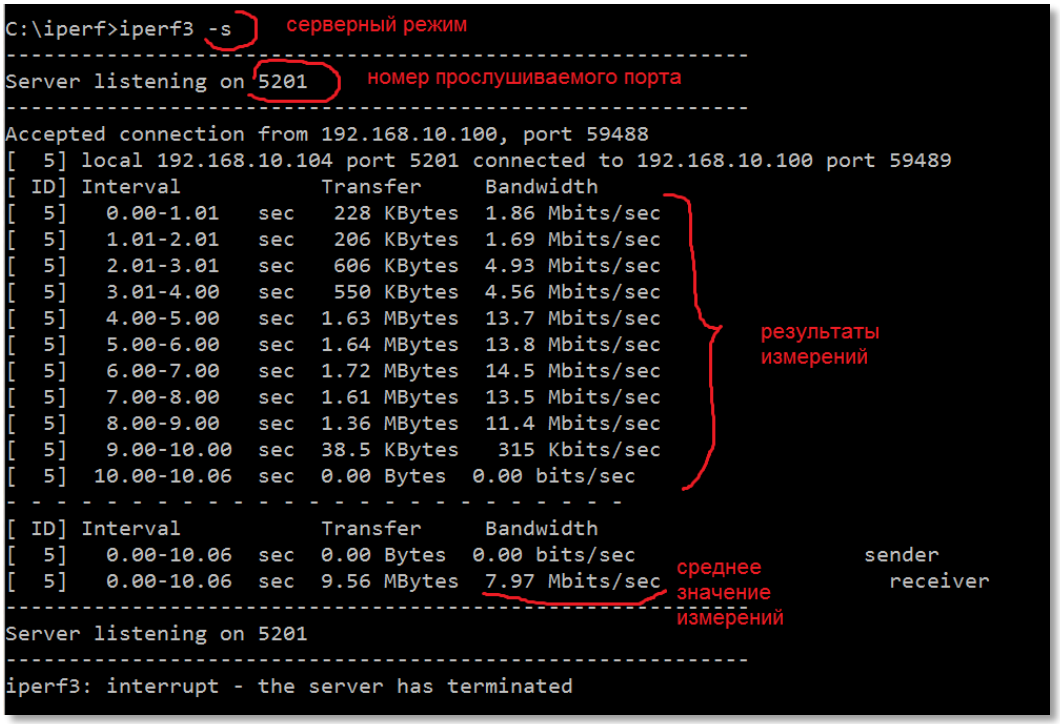
Могут применяться для сетей любых размеров, от PAN до WAN.

Утилита iperf

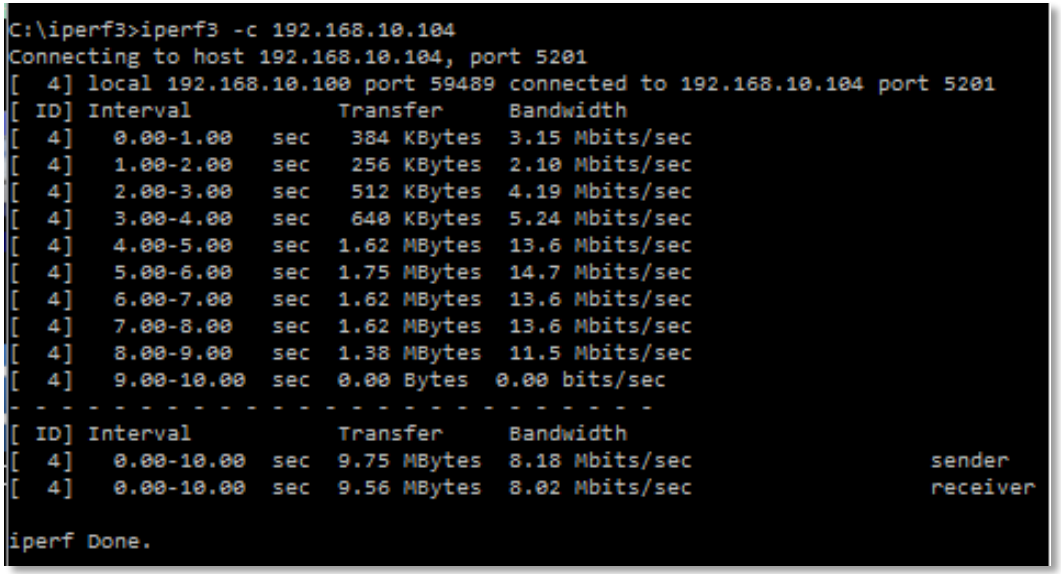
- Утилита iperf не является стандартной утилитой, но часто используется в качестве средства оценки пропускной способности соединения. Представляет собой генератор трафика TCP и UDP, имеет широкий спектр опций, позволяющих проводить гибкую политику оценки пропускной способности.



Утилита также имеет графическую оболочку jperf, облегчающую управление опциями генератора трафика и визуализирую щая результаты измерений.



Пример работы утилиты iperf3 в серверном режиме



Пример работы iperf3 в клиентском режиме

wireshark.org

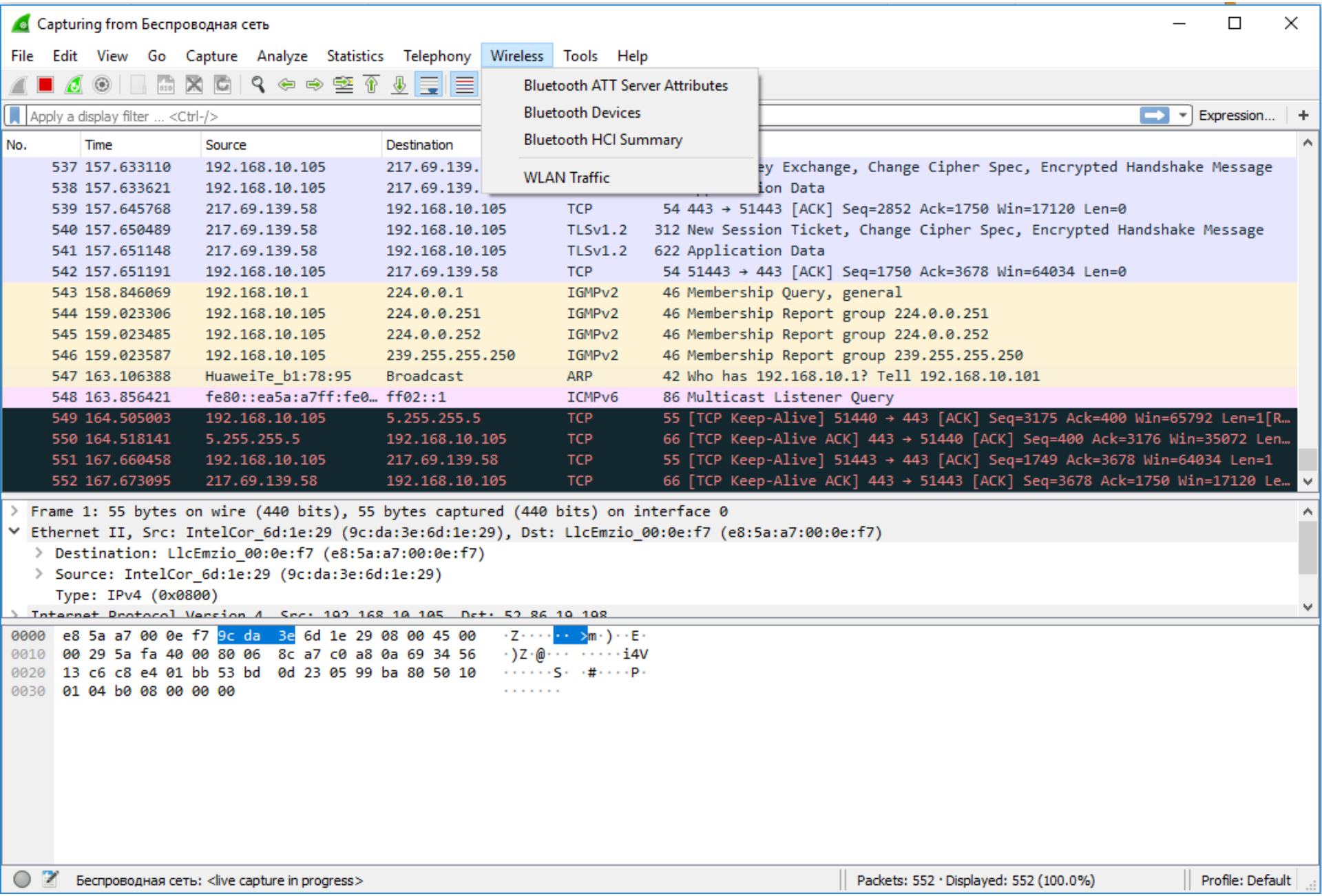
WireShark

Нужный инструмент! Необходимо поставить себе на комп для выполнения лаб и практик. Он бесплатный по умолчанию, но есть платные расширения.

Анализатор трафика, реализуется для ОС Windows (не предоставляет возможность просмотра канального уровня со служебной информацией) и Linux (содержит инструменты для анализа сетей IEEE).

Возможности:

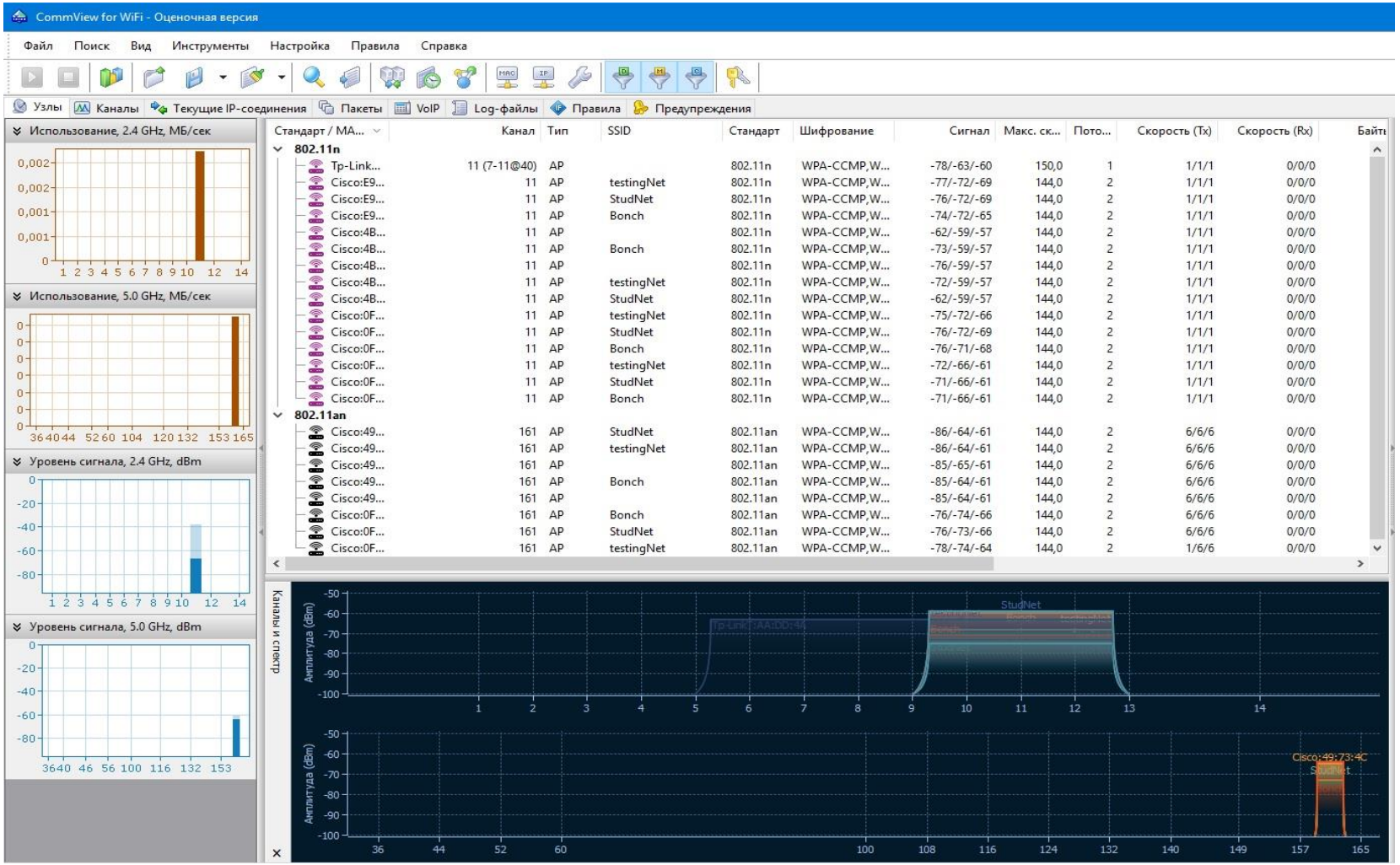
- Анализ структуры пакета вплоть уровня MAC
- Анализ статистических свойств трафика: размеров пакетов, времени прихода пакетов, интенсивности трафика, протоколов и т.п.
- Генератор трафика
- Анализ контента
- Отдельный инструмент для работы с телефонией
- Отдельный инстурмент для работы с беспроводными сетями


Capturing from Беспроводная сеть
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Bluetooth ATT Server Attributes
Bluetooth Devices
Bluetooth HCI Summary
WLAN Traffic
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
537 157.633110 192.168.10.105 217.69.139. ey Exchange, Change Cipher Spec, Encrypted Handshake Message
538 157.633621 192.168.10.105 217.69.139. ion Data
539 157.645768 217.69.139.58 192.168.10.105 TCP 54 443 → 51443 [ACK] Seq=2852 Ack=1750 Win=17120 Len=0
540 157.650489 217.69.139.58 192.168.10.105 TLSv1.2 312 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
541 157.651148 217.69.139.58 192.168.10.105 TLSv1.2 622 Application Data
542 157.651191 192.168.10.105 217.69.139.58 TCP 54 51443 → 443 [ACK] Seq=1750 Ack=3678 Win=64034 Len=0
543 158.846069 192.168.10.1 224.0.0.1 IGMPv2 46 Membership Query, general
544 159.023306 192.168.10.105 224.0.0.251 IGMPv2 46 Membership Report group 224.0.0.251
545 159.023485 192.168.10.105 224.0.0.252 IGMPv2 46 Membership Report group 224.0.0.252
546 159.023587 192.168.10.105 239.255.255.250 IGMPv2 46 Membership Report group 239.255.255.250
547 163.106388 HuaweiTe_b1:78:95 Broadcast ARP 42 Who has 192.168.10.1? Tell 192.168.10.101
548 163.856421 fe80::ea5a:a7ff:fe0… ff02::1 ICMPv6 86 Multicast Listener Query
549 164.505003 192.168.10.105 5.255.255.5 TCP 55 [TCP Keep-Alive] 51440 → 443 [ACK] Seq=3175 Ack=400 Win=65792 Len=1[R…
550 164.518141 5.255.255.5 192.168.10.105 TCP 66 [TCP Keep-Alive ACK] 443 → 51440 [ACK] Seq=400 Ack=3176 Win=35072 Len…
551 167.660458 192.168.10.105 217.69.139.58 TCP 55 [TCP Keep-Alive] 51443 → 443 [ACK] Seq=1749 Ack=3678 Win=64034 Len=1
552 167.673095 217.69.139.58 192.168.10.105 TCP 66 [TCP Keep-Alive ACK] 443 → 51443 [ACK] Seq=3678 Ack=1750 Win=17120 Le…
Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
Ethernet II, Src: IntelCor_6d:1e:29 (9c:da:3e:6d:1e:29), Dst: LlcEmzio_00:0e:f7 (e8:5a:a7:00:0e:f7)
Destination: LlcEmzio_00:0e:f7 (e8:5a:a7:00:0e:f7)
Source: IntelCor_6d:1e:29 (9c:da:3e:6d:1e:29)
Type: IPv4 (0x0800)
0000 e8 5a a7 00 0e f7 9c da 3e 6d 1e 29 08 00 45 00
0010 00 29 5a fa 40 00 80 06 8c a7 c0 a8 0a 69 34 56
0020 13 c6 c8 e4 01 bb 53 bd 0d 23 05 99 ba 80 50 10
0030 01 04 b0 08 00 00 00
Беспроводная сеть: <live capture in progress>
Packets: 552 · Displayed: 552 (100.0%)
Profile: Default

www.tamos.ru

CommView for WiFi

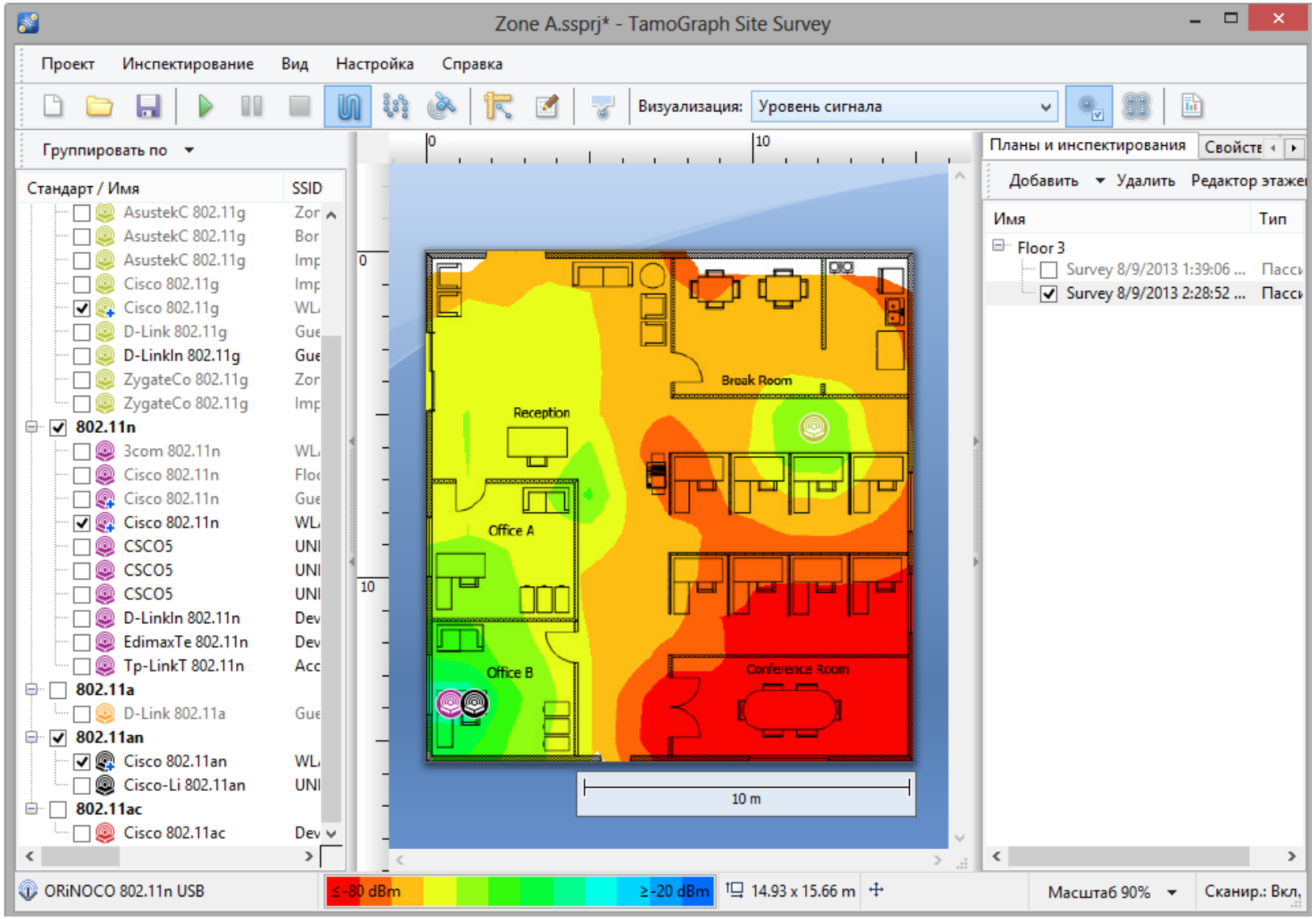
Анализатор трафика для Wi-Fi сетей. Платный, но имеет оценочную версию с ограниченным функционалом



www.tamos.ru

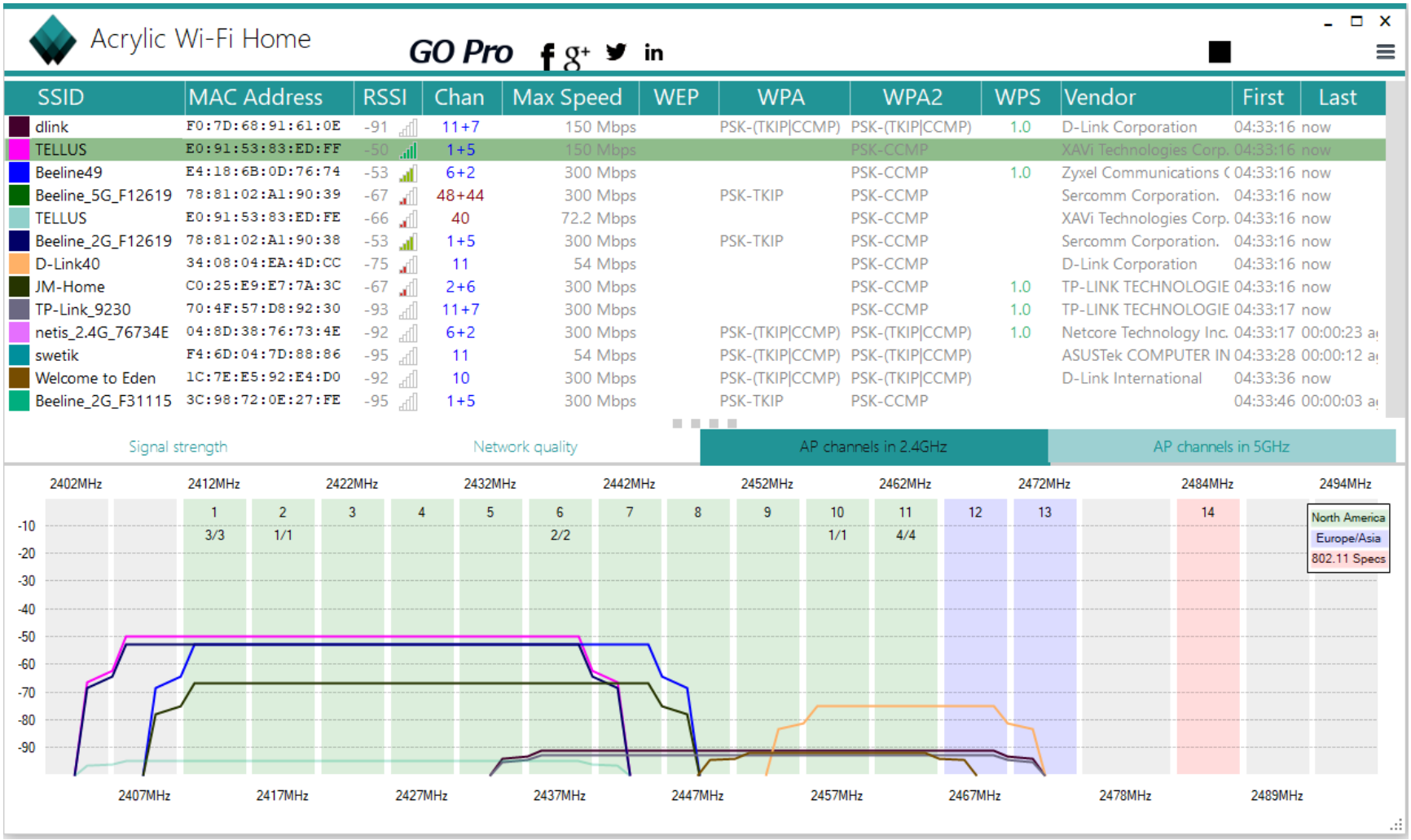
TamoGraph® Site Survey

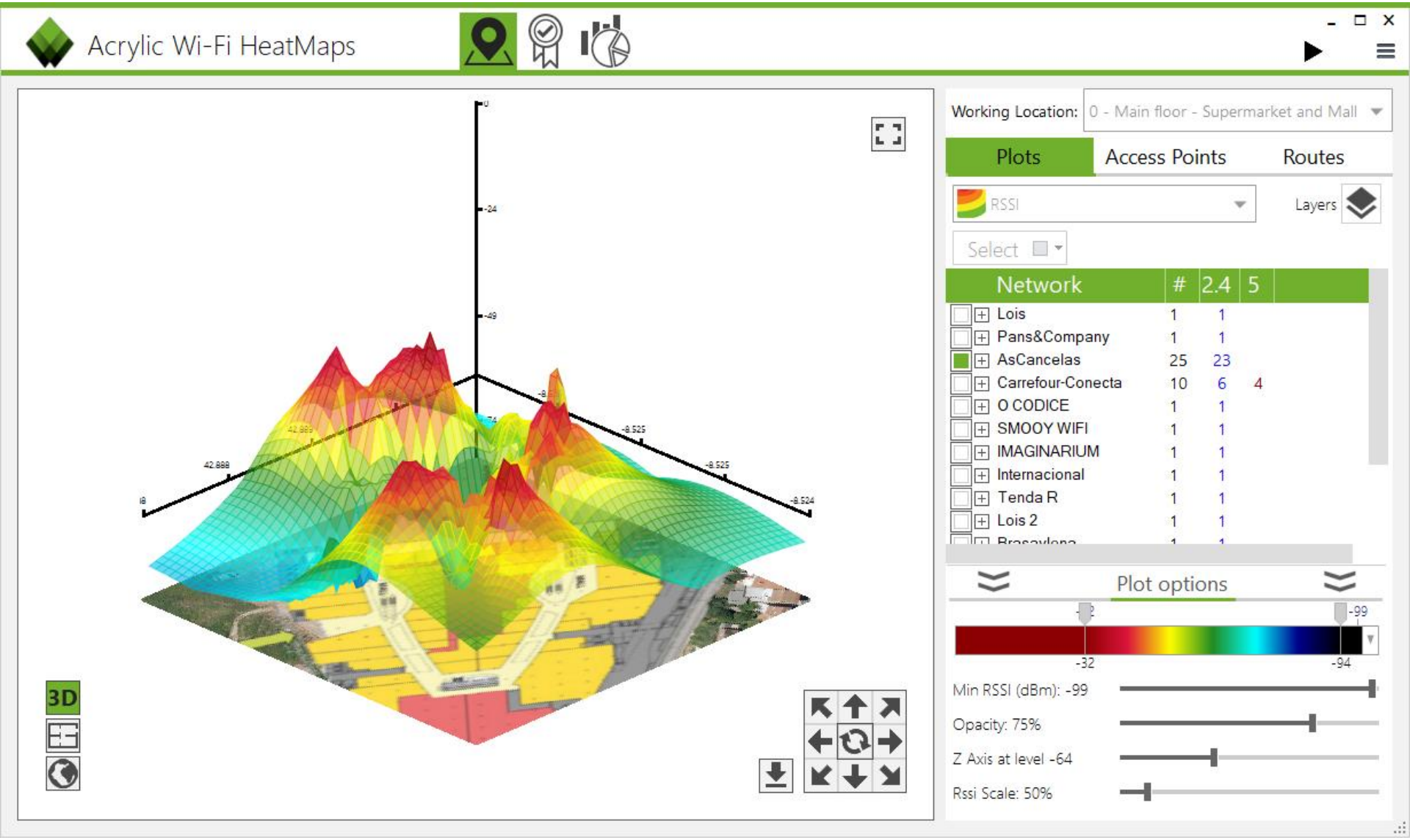
ПО для инспектирования Wi-Fi сетей. Платный, но имеет оценочную версию с ограниченным функционалом



Acrylic Wi-Fi

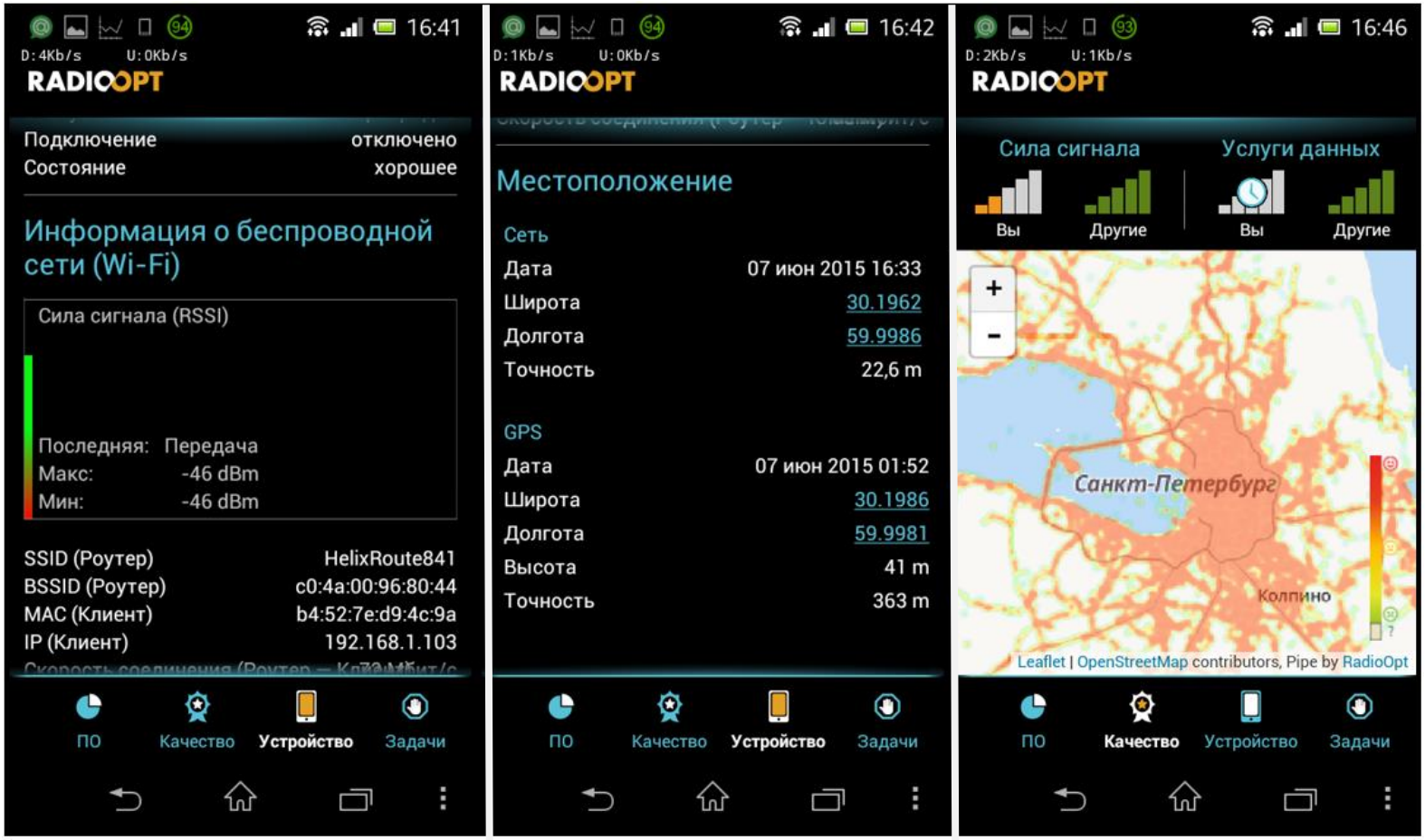
Семейство ПО для анализа Wi-Fi сетей
www.acrylicwifi.com



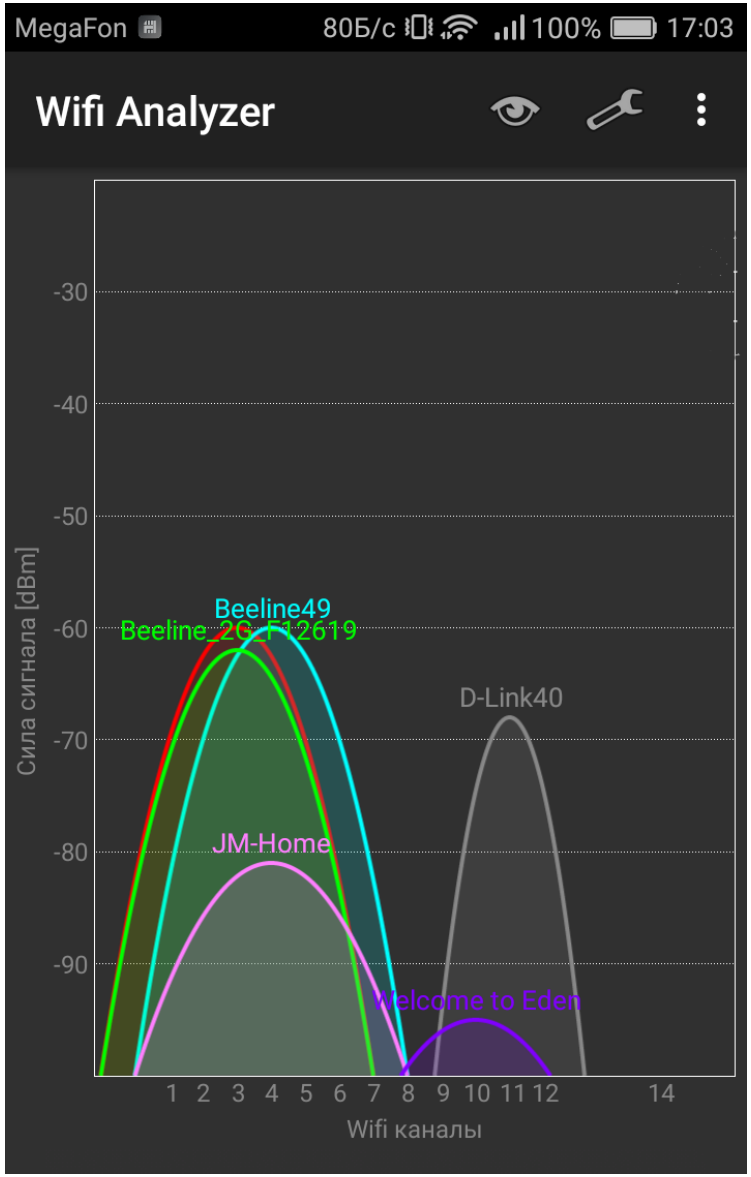

Acrylic Wi-Fi HeatMaps
Working Location:
0 - Main floor - Supermarket and Mall
Plots
Access Points
Routes
RSSI
Layers
Select
Network
#
2.4
5
Lois 1 1
Pans&Company 1 1
AsCancelas 25 23
Carrefour-Conecta 10 6 4
O CODICE 1 1
SMOOY WIFI 1 1
IMAGINARIUM 1 1
Internacional 1 1
Tenda R 1 1
Lois 2 1 1
Plot options
-99
-32
-94
Min RSSI (dBm): -99
Opacity: 75%
Z Axis at level -64
Rssi Scale: 50%
3D

Примеры приложений для телефонов

- Traffic Monitor



Для анализа сетей Wi-Fi



Для анализа сетей мобильной связи