

Прослушивание сетевых сообщений системы стандарта GSM. Часть 2.



Шатилов Евгений, 2 мая 2015г.

Прослушивание сетевых сообщений системы стандарта GSM. Часть 2.

Во второй части курсовой работы будет рассмотрена настройка ПО в среде Linux для приемника RTL-SDR.

1. Установка ОС Linux.

Для работы приемника необходима ОС Linux Xubuntu 14.04.LTS или KALI. Отличие между ними лишь в том, что в KALI имеются уже некоторые установленные модули, в то время как в Xubuntu все придется устанавливать самим. В данной работе используется Linux Xubuntu. На рис. 1. представлены все необходимые модули для работы с приемником:

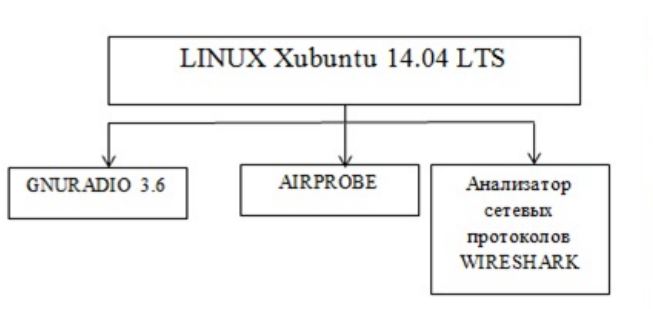


Рис. 1. Модули Linux.

Кратко рассмотрим для чего нужен каждый из модулей:

GNU Radio — это свободная программная утилита под GPL-лицензией для создания программного радио. Она была начата Эриком Блоссом. Она работает для множества различных типов радиоаппаратуры, включая звуковые карты, но в большей степени используется в комбинации с USRP. В основном GNU Radio — это библиотека, содержащая множество стандартных функций обработки сигналов, таких как фильтры и (де)модуляторы.

GNU Radio по умолчанию не содержит специальных средств прослушивания GSM. Однако GNU Radio может быть использовано совместно с другими программными пакетами, такими как *AirProbe* для выполнения низкоуровневых функций прослушивания GSM, таких как приём и демодуляция.

AirProbe — это проект с открытым исходным кодом, пытающийся создать средства интерфейса для GSM (и в будущем возможно 3G) стандартов мобильной связи. Одна из частей проекта работает с приёмом GSM-сигналов (с использованием функций GNU-радио), в то время как другая часть может быть также использована для интерпретации GSM-сигналов.

Wireshark — программа-анализатор трафика для компьютерных сетей Ethernet и некоторых других. Она «знает» структуру самых различных сетевых протоколов, и поэтому позволяет разобрать сетевой пакет, отображая значение каждого поля протокола любого уровня.

Если на компьютере уже стоит другая операционная система, то необходимо установить эмулятор ОС с помощью программы VMWare Player. Скачать ее можно с официального сайта: <http://www.vmware.com/ru>.

2. Установка GNU Radio 3.6.

После установки Linux переходим к установке GNURadio 3.6.

Необходимо открыть домашний каталог из терминала и набрать следующие команды:

```
mkdir gnu-radio-src;
cd gnu-radio-src/;
wget http://www.sbrac.org/files/buil-gnuradio;
cat /etc/debian_version;
```

```
chmod a+x build-gnuradio;
```

```
./build-gnuradio;
```

Начнется процесс установки, который займет около 5 минут. Если возникнут ошибки, связанные с отсутствием связей, необходимо внимательно изучить ошибку и исправить, путем установки недостающих элементов. Перечень всех элементов можно посмотреть набрав команду: `gedit build-gnuradio`.

Следующая команда проверяет наличия приемника rtl-sdr:

```
rtl_test -t;
```

Установка gqrx (тоже самое, что и SDRSharp на Windows):

```
git clone https://github.com/csete/gqrx.git;
```

```
cd gqrx-build-desktop-Qt_4_8_2_in_PATH_System_Release/;
```

`./gqrx` – запуск конфигураций (см. Прослушивание сетевых сообщений системы стандарта GSM. Часть 1. п.3.);

3.Установка Airprobe.

Для установки пакета Airprobe необходимо перейти в созданную ранее директорию в терминале и набрать следующие команды:

```
git clone git://git.gnumonks.org/airprobe.git;
```

```
cd airprobe/gsmdecode;
```

```
./bootstrap;
```

```
./configure;
```

```
make;
```

```
cd airprobe/gsm-receiver;
```

```
./bootstrap;
```

```
./configure;
```

```
make;
```

Если у вас не работает команда `git clone`, возможно вместо нее необходимо набрать `wget`.

4.Установка Wireshark.

Установка Wireshark происходит из центра ПО убунту (Ubuntu Software Center) рис.2.

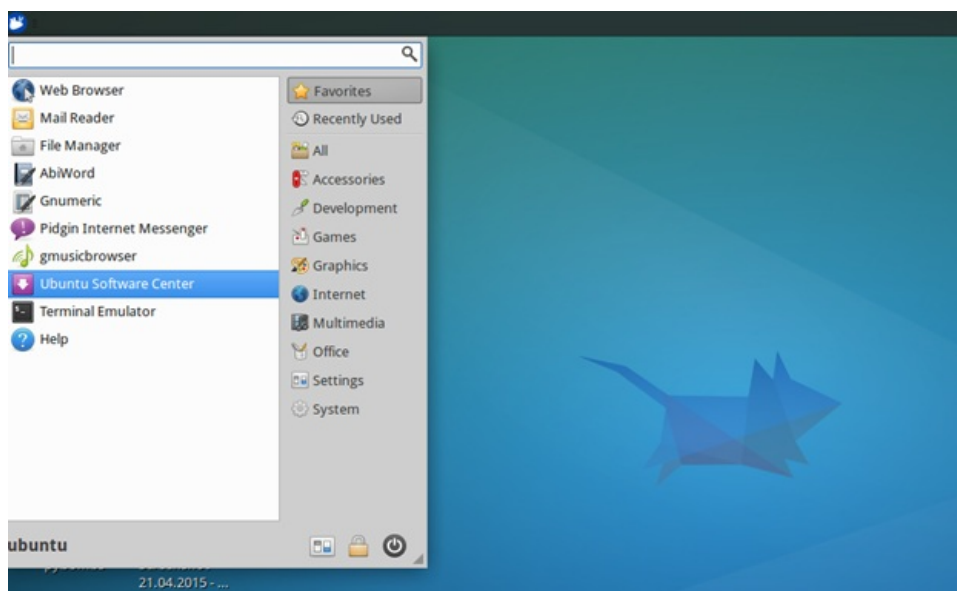


Рис.2. Ubuntu Software Center.

Щелкнуть на нем левой кнопкой мыши. В открытом окне набрать в поиске Wireshark. После того как программа произведет поиск, необходимо найти нужный пакет и нажать кнопку Install.

Т.О. Были рассмотрены модули для работы приемника rtl-sdr, их назначение и установка.

Список литературы:

1. <http://www.securitylab.ru/analytics/448062.php>;
2. <http://rus-linux.net/nlib.php?name=/MyLDP/lvs/wireshark/wireshark.html>;
3. <http://www.rtl-sdr.com/rtl-sdr-tutorial-analyzing-gsm-with-airprobe-and-wireshark/>;
4. https://ru.wikipedia.org/wiki/GNU_Radio;
5. <https://www.pgpru.com/biblioteka/statji/eavesdroppingongsm/theopensourcepracticalimplementation>;
6. <https://ru.wikipedia.org/wiki/Wireshark>.



Статья опубликована на сайте Omoled.ru - Образовательные сообщества
Ссылка на статью: <http://omoled.ru/publications/view/721>