Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования
«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ» (ТУСУР)
Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)

УТВЕРЖДАЮ
заведующий каф. КИБЭВС
_____А.А. Шелупанов
«_____»_____2015г.

ПАССИВНЫЙ ПЕРЕХВАТ ПАКЕТОВ ПО БЕСПРОВОДНОЙ СЕТИ ИНТЕРНЕТ (WI-FI)

Курсовая работа по дисциплине «Безопасность сетей ЭВМ»
Пояснительная записка

Выполнила:
студентка гр. 722
_____М.В. Мейта
«_____»_____2015г.

Научный руководитель:
аспирант каф. КИБЭВС
_____А.К. Новохрестов
«_____»_____2015г.

Томск 2015

РЕФЕРАТ

Курсовая работа содержит 18 страниц, 21 рисунков, 0 таблиц, 2 источника, 0 приложение.

RASPBERRY PI, UBUNTU, WI-FI, TCPDUMP, PCAP, RASPBIAN, WIRESHARK, BASH, СНИФФЕР, СЕТЕВОЙ ТРАФИК.

Цель работы — разработать и настроить систему пассивного перехвата пакетов по беспроводной сети Интернет (Wi-Fi) в научно-образовательных целях.

Проект выполнен с использованием следующих программных и аппаратных средств:

– ОС Linux Ubuntu 15.04;

– ОС Linux Raspbian Jessie Light 4.1;

– Wi-Fi-адаптер TP-Link TL-WN722NC;

– tcpdump — консольная утилита Unux для перехвата и анализа сетевого трафика;

– Wireshark — программа-анализатор сетевого трафика с графическим пользовательским интерфейсом.

Пояснительная записка выполнена при помощи системы компьютерной вёрстки LaTeX.

Содержание

Введение

Беспроводные сети небезопасны, особенно открытые. Но и зашифрованные не являются на 100

тут надо сочинение на эту тему

склепать сниффер

В качестве задания на курсовую работу была поставлена задача разработать пассивный перехватчик пакетов на базе Raspberry Pi. **????**

Задачи: установить настроить сниффить анализировать

1 Используемые прораммные и аппаратные средства, обоснование выбора и их описание

1.1 Raspberry Pi + TPLink

1.2 Ubuntu

1.3 Raspbian

1.4 tcpdump

1.5 wireshark

2 Проектирование и настройка пакетного сниффера

2.1 Установка ОС Raspbian

Для установки оперционной системмы Raspbian на Raspberry Pi необходимо перейти на страницу загрузок на официальном сайте [1] и скачать необходимый образ ОС (рис. 2.1), затем установить загруженный образ на SD-карту, которая впоследствии будет подключена к Raspberry Pi и с которой непосредственно будет загружаться система.

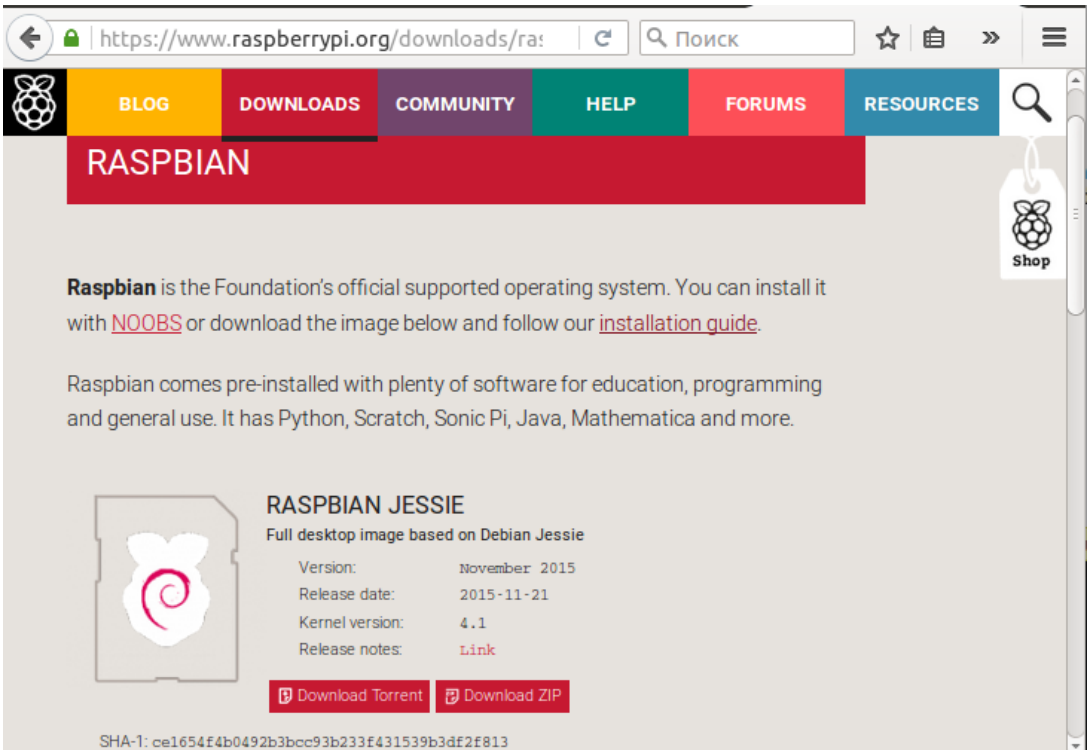

Рисунок 2.1 – Официальная страница загрузок ОС Raspbian

Инструкцию по установке образа системы на SD-карту можно найти, перейдя по ссылке [2].

После распаковки заргуженного архива с образом системы, необходимо вставить SD-карту в слот и выполнить следующие команды:

```
$ df -h   # увидеть все примонтированные устройства
$ umount /dev/<ИМЯ_УСТРОЙСТВА>    # отмонтировать SD-карту
$ dd bs=4M if=2015-11-21-raspbian-jessie.img of=/dev/sdd    # записать образ
$ sync
```

Далее достаточно извлечь SD-карту и установить ее в соответсвующий разъем Raspberry Pi.

2.2 настройка сети (Ethernet)

Все остальные настройки оставить по умолчанию.

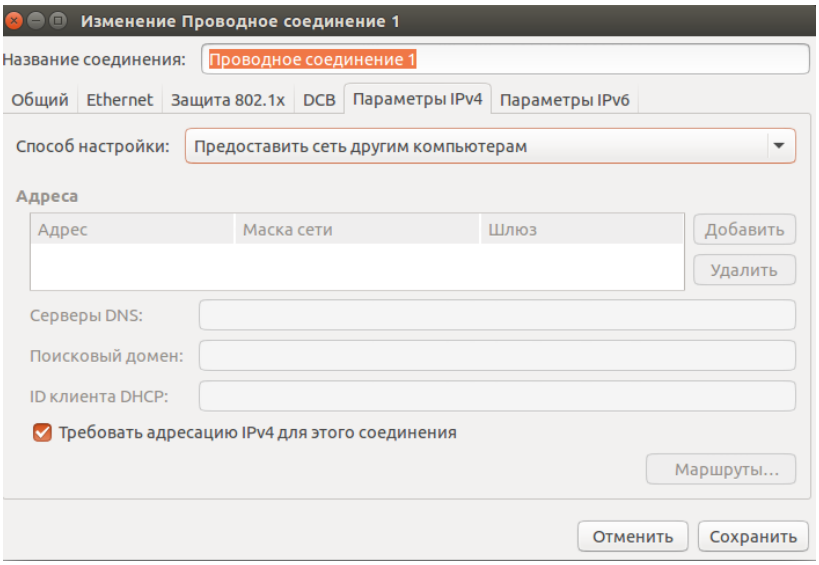

Рисунок 2.2 – Параметры IPv4 для проводного соединения

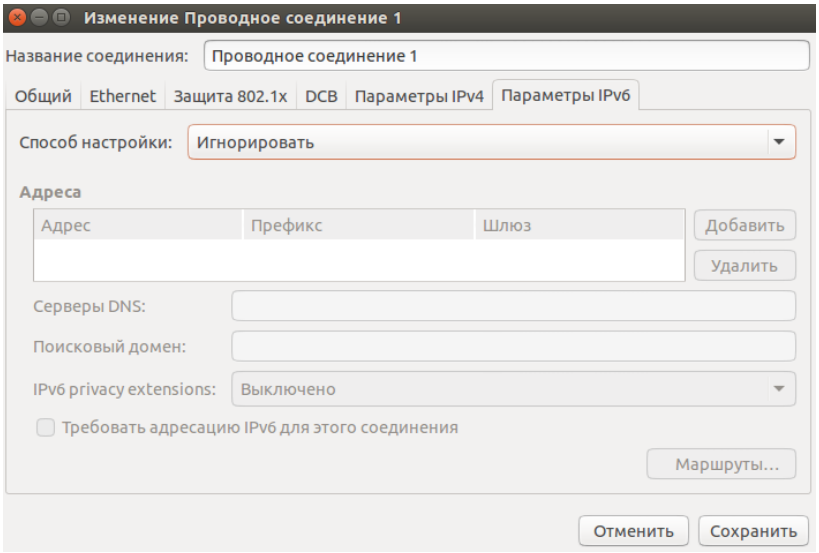

Рисунок 2.3 – Параметры IPv6 для проводного соединения

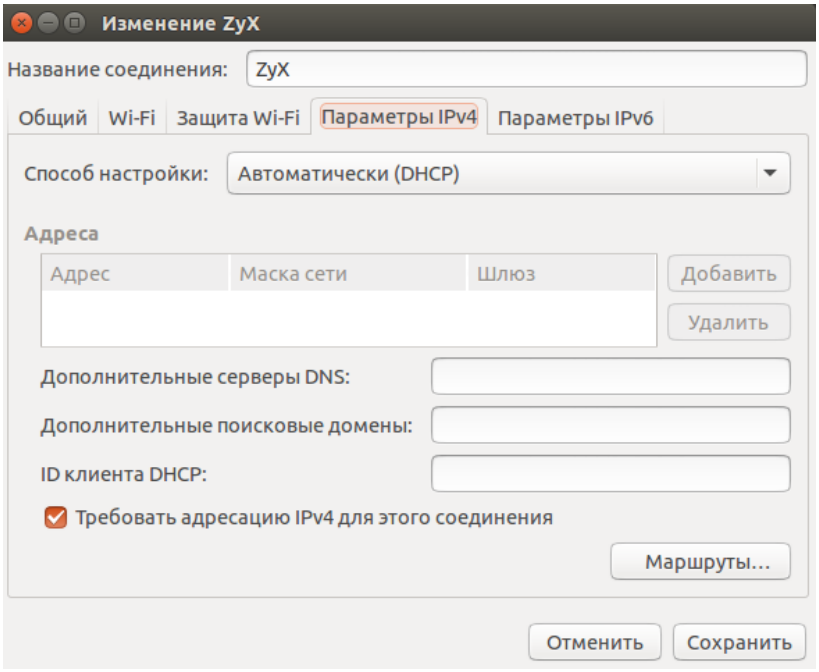

Рисунок 2.4 – Параметры IPv4 для беспроводного соединения

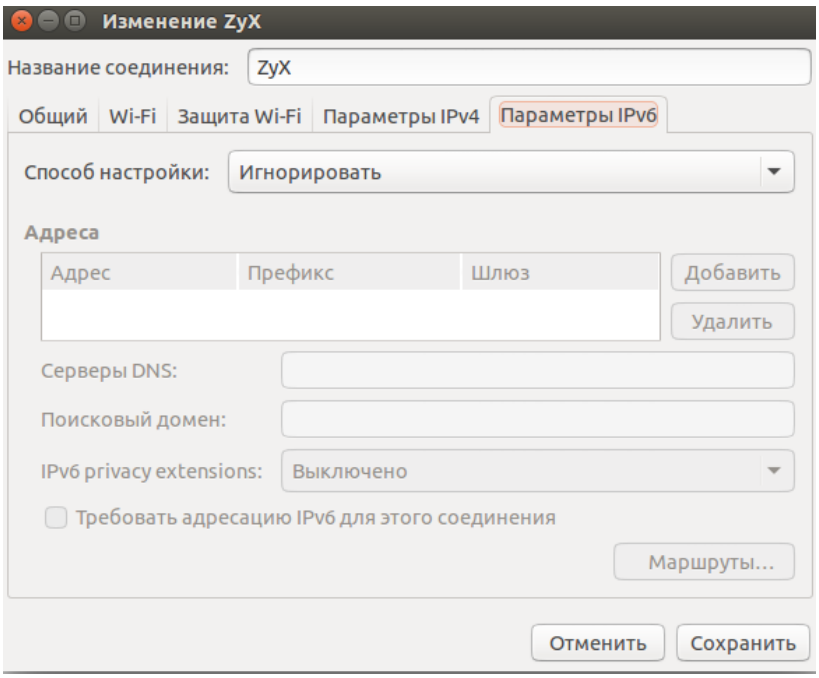

Рисунок 2.5 – Параметры IPv6 для беспроводного соединения

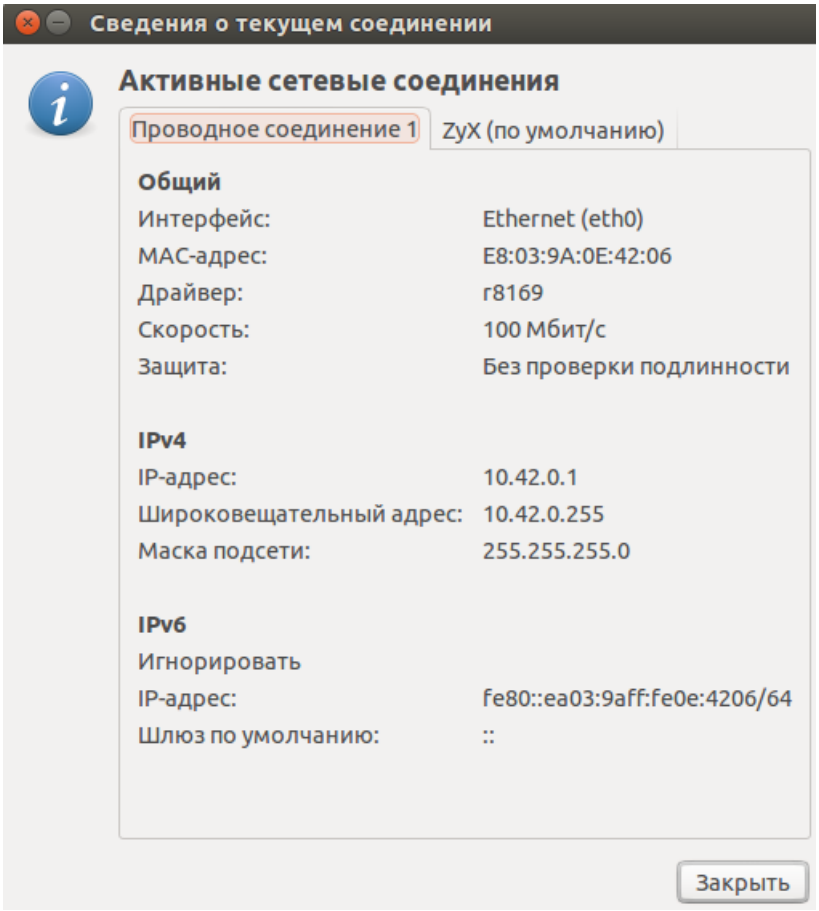

Рисунок 2.6 – Сведения о проводном соединении

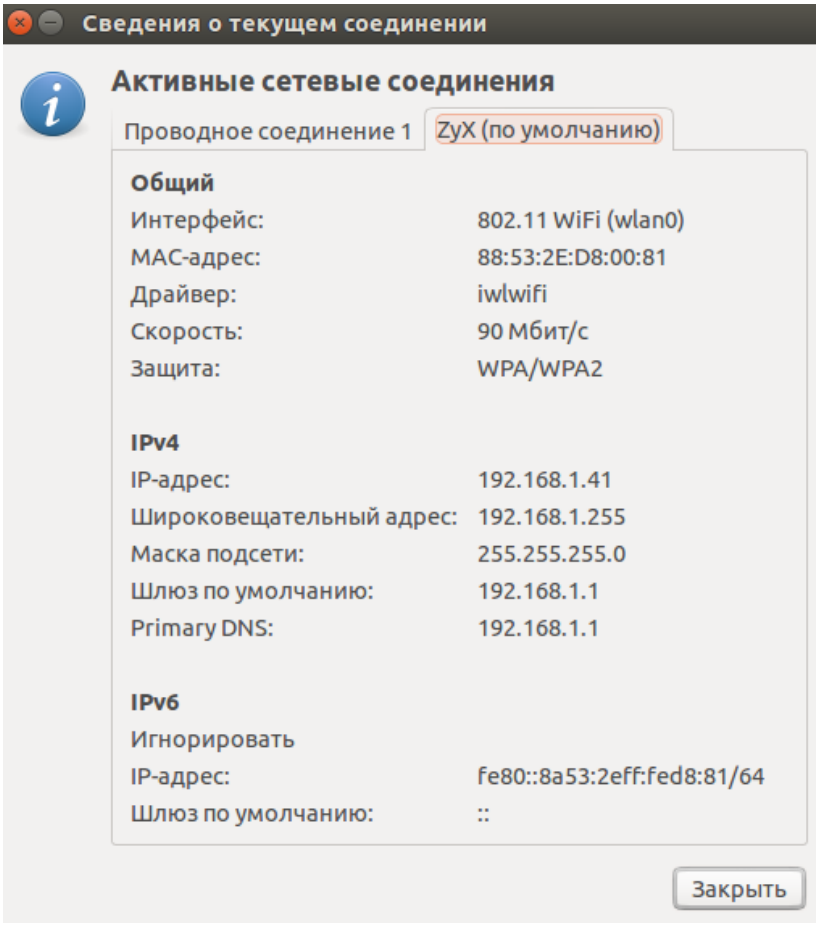

Рисунок 2.7 – Сведения о беспроводном соединении

2.3 Установка ssh-соединения

arp -vn:

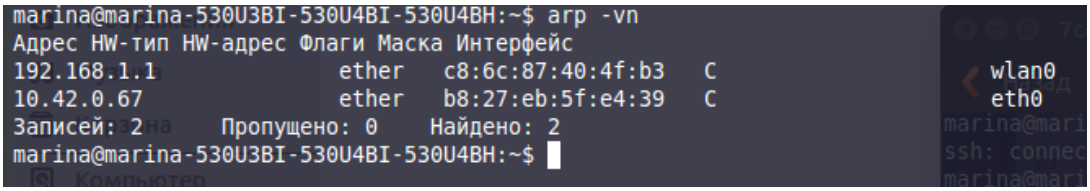

Рисунок 2.8 – Параметры IPv4 для проводного соединения

connect ssh:

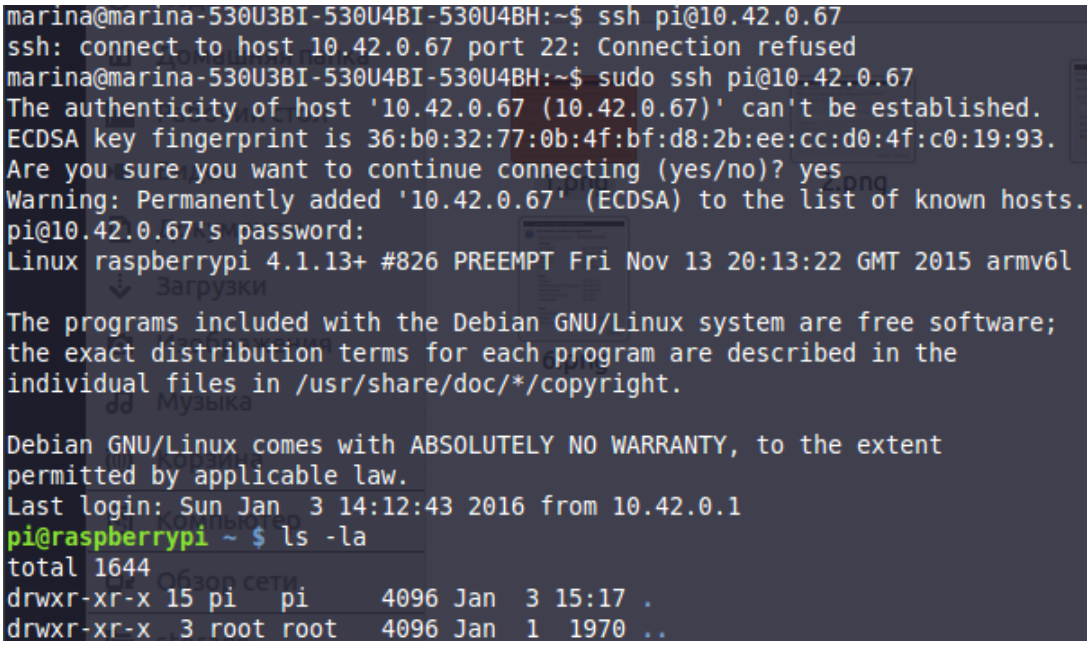

Рисунок 2.9 – Параметры IPv4 для проводного соединения

все,мы в системе

2.4 Установка драйвера TP-Link

Узнаем версию системы и проверяем устройства USB

```
pi@raspberrypi / $ uname -a
Linux raspberrypi 4.1.13+ #826 PREEMPT Fri Nov 13 20:13:22 GMT 2015 armv6l GNU/Linux
```

Рисунок 2.10 – Узнаем версию системы

```
pi@raspberrypi / $ lsusb
Bus 001 Device 002: ID 0424:9512 Standard Microsystems Corp.
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 003: ID 0424:ec00 Standard Microsystems Corp.
Bus 001 Device 004: ID 0bda:8179 Realtek Semiconductor Corp.
```

Рисунок 2.11 – проверяем устройства USB

тут ссылка на то,как устанавливать драйвер согласно версии системы https://www.raspberrypi.org/forums/viewtopic.php?p=462982

Скачиваем драйвер:

```
pi@raspberrypi ~ $ wget https://dl.dropboxusercontent.com/u/80256631/8188eu-20151113.tar.gz
--2016-01-03 16:26:02--  https://dl.dropboxusercontent.com/u/80256631/8188eu-20151113.tar.gz
Resolving dl.dropboxusercontent.com (dl.dropboxusercontent.com)... 199.47.217.69
Connecting to dl.dropboxusercontent.com (dl.dropboxusercontent.com)|199.47.217.69|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 416724 (407K) [application/octet-stream]
Saving to: `8188eu-20151113.tar.gz'

100%[======================================================================================================>]

2016-01-03 16:26:11 (221 KB/s) - `8188eu-20151113.tar.gz' saved [416724/416724]
```

Рисунок 2.12 – Скачиваем драйвер

установим и ребутнемся

```
pi@raspberrypi ~ $ tar -zxvf 8188eu-20151113.tar.gz
8188eu.ko
8188eu.conf
install.sh
pi@raspberrypi ~ $ ./install.sh
sudo cp 8188eu.conf /etc/modprobe.d/.
sudo install -p -m 644 8188eu.ko /lib/modules/4.1.13+/kernel/drivers/net/wireless
sudo depmod 4.1.13+

Reboot to run the driver.

If you have already configured your wifi it should start up and connect to your
wireless network.

If you have not configured your wifi you will need to do that to enable the wifi.
pi@raspberrypi ~ $ sudo reboot
```

Рисунок 2.13 – Устанавливаем драйвер

Проверим командой ifconfig

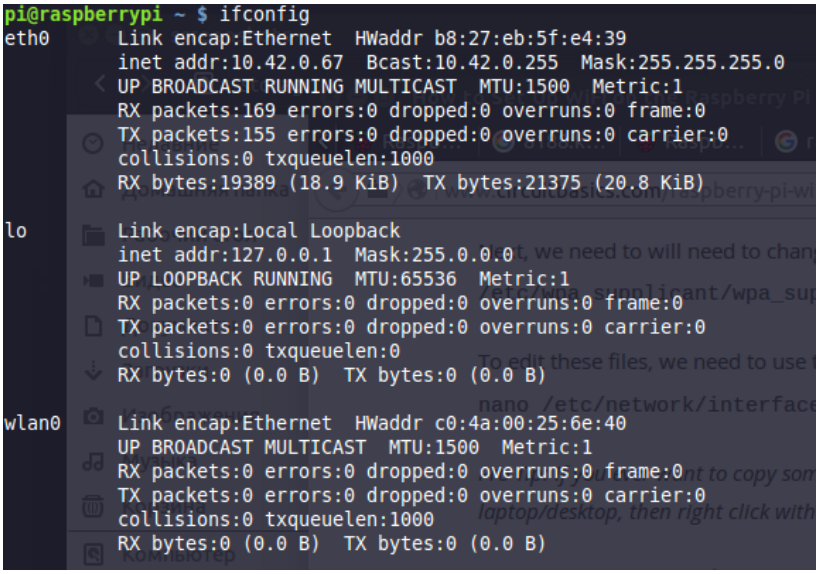

Рисунок 2.14 – ifconfig

2.5 Настройка режима monitor mode

Для начала попробуем установить Wi-Fi соединение и подсоединиться к RPi без Ethernet-соединения.

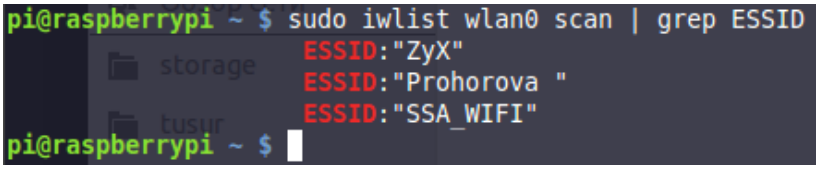

Рисунок 2.15 – просканировали сеть

Рисунок 2.16 – путь к config

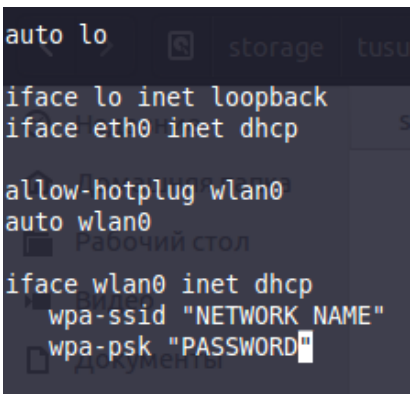

Рисунок 2.17 – config

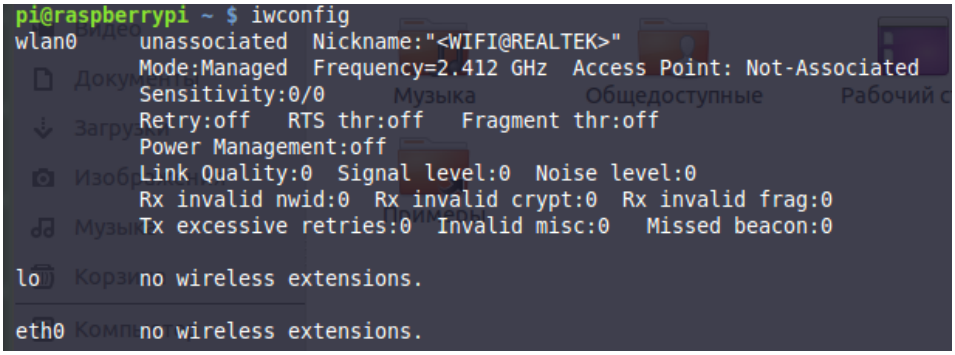

Рисунок 2.18 – config

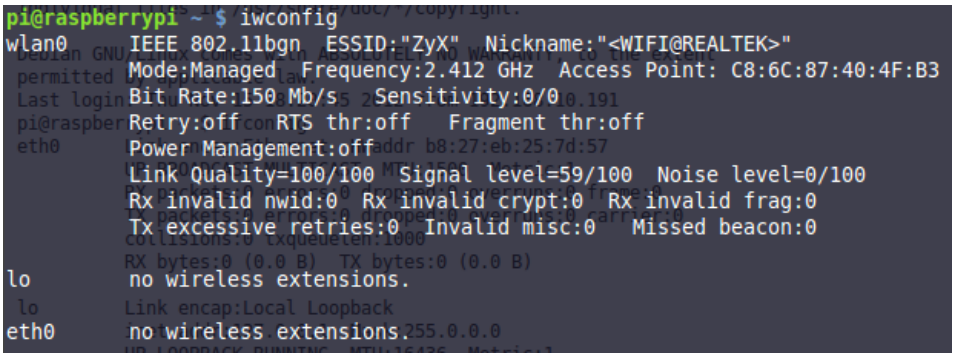

Рисунок 2.19 – config

подняли сетку в режиме Managed

тут можно рассказать про разные режимы даптеров (их 6) и про мониторящий режим. Устройство может в определенный момент времени находиться только в одном режиме.

Настроим адаптер в режим приема пакетов. Для этого необходимо ввести команду sudo iwconfig wlan0 mode monitor При попытке ввести данную команду видим следующее сообщение:

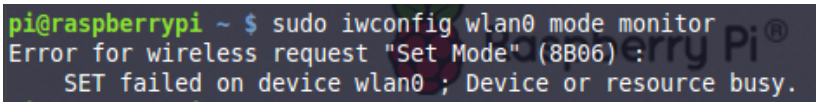

Рисунок 2.20 – ресурс занят

это связано с тем, что в системе работает network interface plugging daemon (ссылка на распберри пи орг) необходимо его отключить для того, чтобы перевести устройство в другой режим работы

напишем небольшой bash-скрипт, который будет переводить адаптер в режим перехвата пакетов и содержать следующие команды: sudo service ifplugd stop останавливаем работу демона sudo ifconfig wlan0 down отключаем wi-fi соединение sudo iwconfig wlan0 mode monitor включаем прослушивающий режим sudo ifconfig wlan0 up включаем wi-fi соединение sudo service ifplugd start запускаем демона iwconfig проверям настройки

результат работы скрипта приведен на рисунке ... Устройство теперь в режиме перехвата пакетов. Данный скрипт необходимо запускать снова при перезапуске системы, поскольку по умолчанию устройство переходит в режим managed

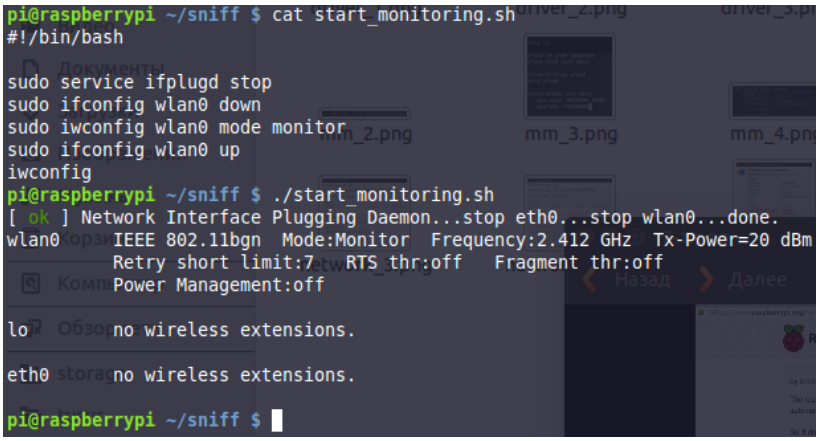

Рисунок 2.21 – результат выполнения скрипта

2.6 tcpdump

2.7 wireshark

Заключение

Список использованных источников

1 Raspbian [Электронный ресурс]. URL: https://www.raspberrypi.org/downloads/raspbian/ (дата обращения: 25.09.2015).

2 Installing Operating System Images on Linux [Электронный ресурс]. URL: https://www.raspberrypi.org/documentation/installation/installing-images/README.md (дата обращения: 25.09.2015).