

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

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

Курсовая работа по дисциплине «Безопасность сетей ЭВМ»

Выполнила:
студентка гр.722 каф. КИБЭВС
Мейта Марина
Руководитель:
аспирант каф. КИБЭВС
Новохрестов А.К.

Что такое сниффер?

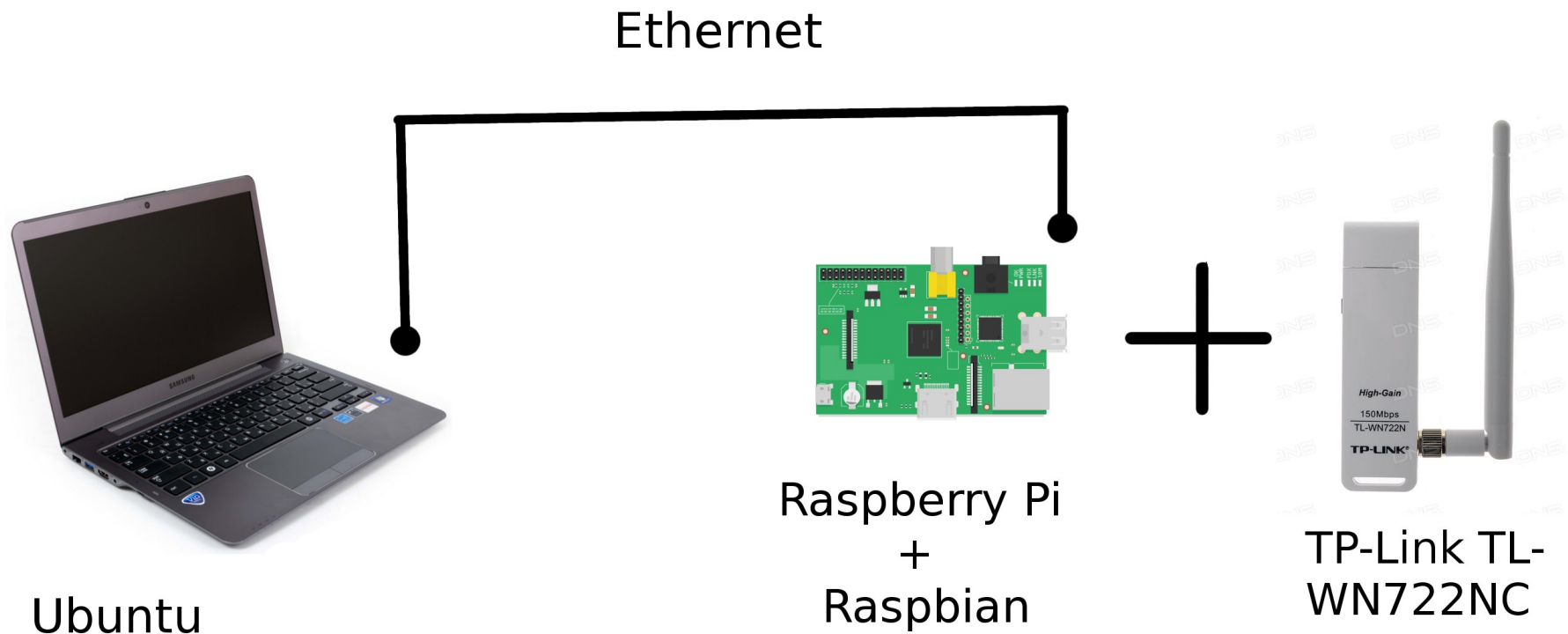


ВЫПОЛНЕНИЕ РАБОТЫ ПРОИЗВОДИЛОСЬ ИСКЛЮЧИТЕЛЬНО В
НАУЧНО-ОБРАЗОВАТЕЛЬНЫХ ЦЕЛЯХ

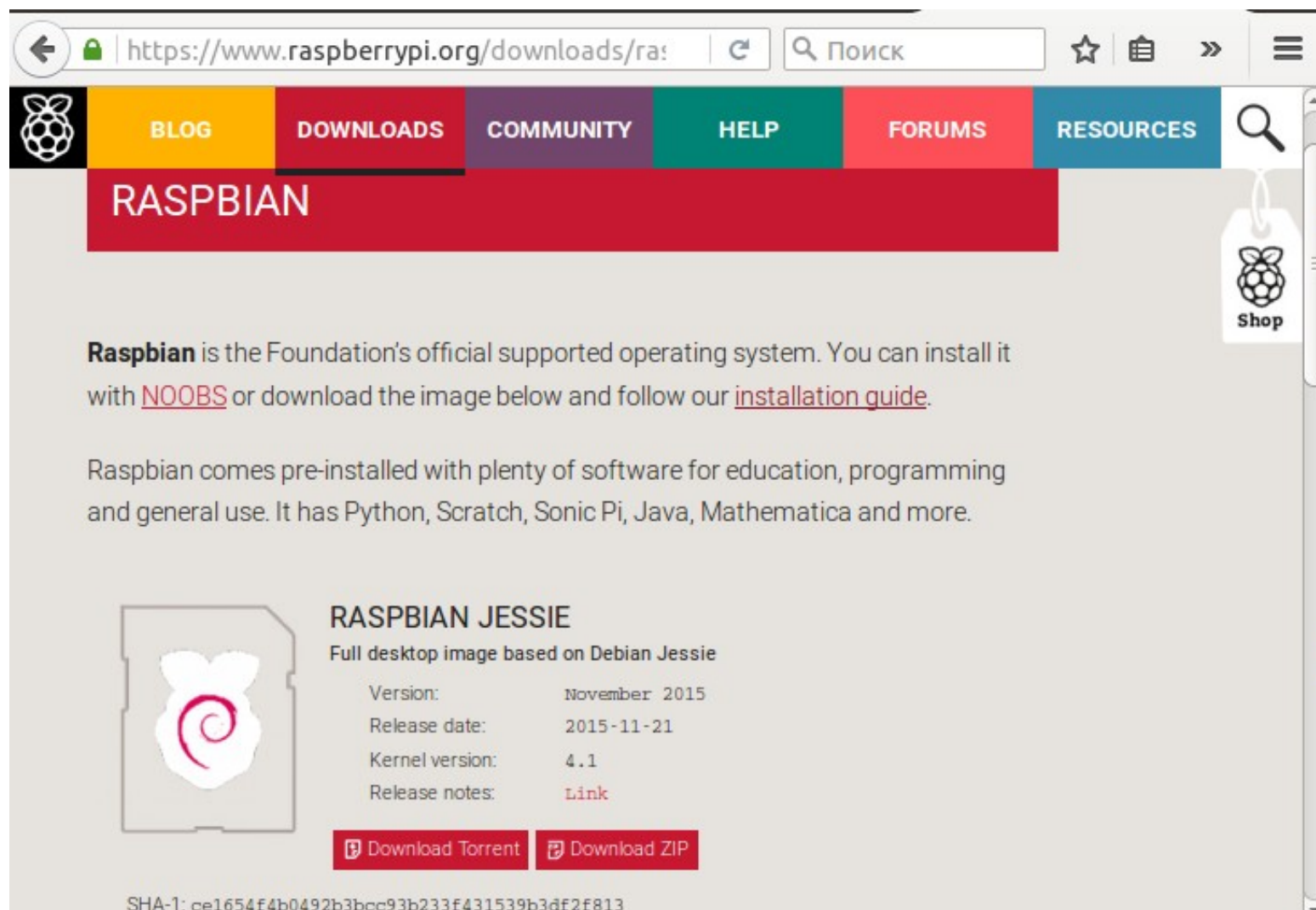
Что такое сниффер?

- «to sniff» — «нюхать»
- пассивные и активные снифферы
- ARP-spoofing (ARP — poisoning) — разновидность сетевой атаки типа MITM (англ. Man in the middle)
- Шифрованный трафик != безопасная сеть
- Открытые сети Wi-Fi-доступа — тем более

Необходимые устройства



Установка Raspbian



The screenshot shows the Raspbian website's download page. The browser's address bar displays the URL <https://www.raspberrypi.org/downloads/raspbian>. The website's navigation bar includes links for BLOG, DOWNLOADS, COMMUNITY, HELP, FORUMS, and RESOURCES. A large red banner with the word "RASPBIAN" is prominently displayed. Below this, a paragraph states: "Raspbian is the Foundation's official supported operating system. You can install it with [NOOBS](#) or download the image below and follow our [installation guide](#)." Another paragraph mentions: "Raspbian comes pre-installed with plenty of software for education, programming and general use. It has Python, Scratch, Sonic Pi, Java, Mathematica and more." The main content area features a section for "RASPBIAN JESSIE", described as a "Full desktop image based on Debian Jessie". To the left of this section is an image of a SD card with the Raspbian logo. To the right, a table lists the following details:

Version:	November 2015
Release date:	2015-11-21
Kernel version:	4.1
Release notes:	Link

Below the table are two red buttons: "Download Torrent" and "Download ZIP". At the bottom of the page, the SHA-1 hash is provided: "SHA-1: ce1654f4b0492b3bcc93b233f431539b3df2f813".

Запись образа

- `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`

Настройка проводного соединения

Изменение Проводное соединение 1

Название соединения: **Проводное соединение 1**

Общий Ethernet Защита 802.1x DCB **Параметры IPv4** Параметры IPv6

Способ настройки: **Предоставить сеть другим компьютерам**

Адреса

Адрес	Маска сети	Шлюз	
			Добавить
			Удалить

Серверы DNS:

Поисковый домен:

ID клиента DHCP:

☒ **Требовать адресацию IPv4 для этого соединения**

Маршруты...

Отменить Сохранить

Настройка проводного соединения

Изменение Проводное соединение 1

Название соединения: Проводное соединение 1

Общий Ethernet Защита 802.1x DCB Параметры IPv4 Параметры IPv6

Способ настройки: Игнорировать

Адреса

Адрес	Префикс	Шлюз	Добавить
			Удалить

Серверы DNS:

Поисковый домен:

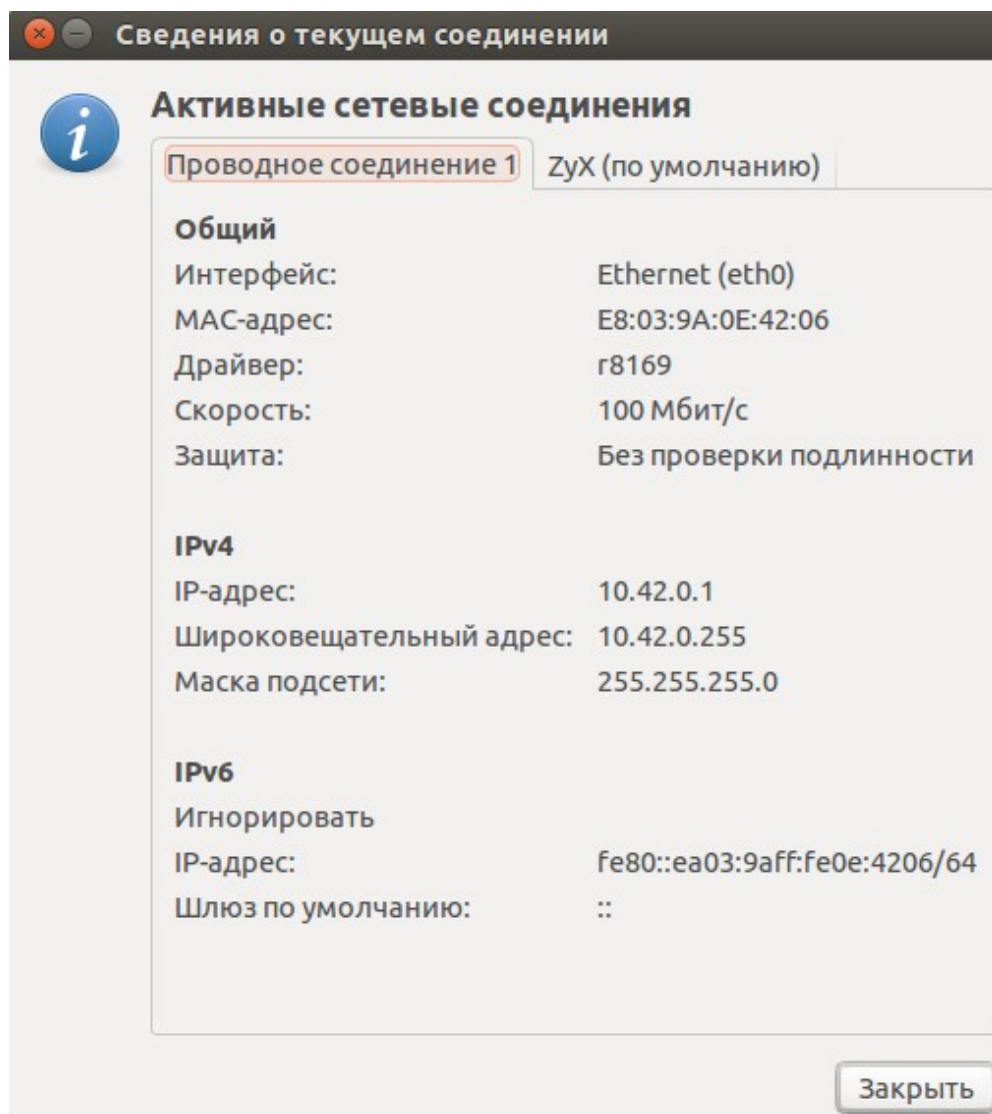
IPv6 privacy extensions: Выключено

☐ Требовать адресацию IPv6 для этого соединения

Маршруты...

Отменить Сохранить

Настройка проводного соединения



Установка ssh-соединения

- arp -vn
- ssh pi@10.42.0.67

```
marina@marina-530U3BI-530U4BI-530U4BH:~$ arp -vn
Адрес HW-тип HW-адрес Флаги Маска Интерфейс
192.168.1.1      ether  c8:6c:87:40:4f:b3  C
10.42.0.67      ether  b8:27:eb:5f:e4:39  C
Записей: 2 на   Пропущено: 0   Найдено: 2
marina@marina-530U3BI-530U4BI-530U4BH:~$
```

```
wlan0
eth0
marina@mari
ssh: connec
marina@mari
```

Установка драйвера TP-Link

- Версия ОС
- ID USB Device

```
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.
```

Режим перехвата пакетов

- /etc/network/interfaces
- стандарт WNIC 802.11master, **managed**, ad-hoc, mesh, repeater, **monitor**
- Устройство одновременно может работать только в одном режиме
- `sudo iwconfig wlan0 mode monitor`

```
pi@raspberrypi ~ $ sudo iwconfig wlan0 mode monitor
Error for wireless request "Set Mode" (8B06) :
    SET failed on device wlan0 ; Device or resource busy.
```

Network Interface Plugging Daemon

```
$ #!/bin/bash
$ 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 #проверяем настройки
```

iwconfig «before»

```
pi@raspberrypi ~$ iwconfig
wlan0 IEEE 802.11bgn ESSID:"ZyX" Nickname:"<WIFI@REALTEK>"
Mode:Managed Frequency:2.412 GHz Access Point: C8:6C:87:40:4F:B3
Bit Rate:150 Mb/s Sensitivity:0/0
Retry:off RTS thr:off Fragment thr:off
Power Management:off
Link Quality=100/100 Signal level=59/100 Noise level=0/100
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
Tx excessive retries:0 Invalid misc:0 Missed beacon:0
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

lo
no wireless extensions.

lo
Link encap:Local Loopback

eth0
no wireless extensions.255.0.0.0
```

iwconfig «after»

```
pi@raspberrypi ~/sniff $ cat start_monitoring.sh
#!/bin/bash

sudo service ifplugd stop
sudo ifconfig wlan0 down
sudo iwconfig wlan0 mode monitor
sudo ifconfig wlan0 up
iwconfig

pi@raspberrypi ~/sniff $ ./start_monitoring.sh
[ ok ] Network Interface Plugging Daemon...stop eth0...stop wlan0...done.
wlan0 IEEE 802.11bgn Mode:Monitor Frequency:2.412 GHz Tx-Power=20 dBm
        Retry short limit:7 RTS thr:off   Fragment thr:off
        Power Management:off

lo no wireless extensions.

eth0 no wireless extensions.

pi@raspberrypi ~/sniff $
```

Рсар-файл

sniff.pcap [Wireshark 1.12.1 (Git Rev Unknown from unknown)]

Filter: Expression... Clear

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	ZyxelCom 4e:7e:02	Broadcast	802.11	222	Beacon frame

► Frame 1: 222 bytes on wire (1776 bits), 222 bytes captured (1776 bits)

► Radiotap Header v0, Length 36

- Header revision: 0
- Header pad: 0
- Header length: 36
- Present flags
 - MAC timestamp: 58444392
- Flags: 0x10
 - Data Rate: 1,0 Mb/s
 - Channel frequency: 2412 [BG 1]
- Channel type: 802.11b (0x00a0)
 - SSI Signal: -51 dBm

Offset	Hex	ASCII
0000	00 00 24 00 2f 40 00 a0 20 08 00 00 00 00 00 00	..\$./@..
0010	68 ca 7b 03 00 00 00 00 10 02 6c 09 a0 00 cd 00	h.{..... ..l.....
0020	00 00 bb 00 80 00 00 00 ff ff ff ff ff ff cc 5d].....
0030	4e 4e 7e 02 cc 5d 4e 4e 7e 02 b0 ef 76 e1 6c c1	NN~..]NN ~...v.l.
0040	1e 00 00 00 64 00 11 04 00 04 68 6f 6d 65 01 08	...d... ..home..
0050	82 84 8b 96 92 a4 c8 ec 03 01 01 32 04 8c 98 b02....
0060	e0 07 06 54 57 20 01 0d 14 dd 27 00 50 f2 04 10	...TW'.P...
0070	4a 00 01 10 10 44 00 01 02 10 47 00 10 28 80 28	J....D.. ..G..(.
0080	80 28 80 18 80 a8 80 cc 5d 4e 4e 7e 02 10 3c 00	.(.....]NN~..<.
0090	01 01 05 04 00 01 00 00 2a 01 04 dd 1a 00 50 f2 *.....P.
00a0	01 01 00 00 50 f2 02 02 00 00 50 f2 02 00 50 f2P... ..P...P.
00b0	04 01 00 00 50 f2 02 30 18 01 00 00 0f ac 02 02P..0
00c0	00 00 0f ac 02 00 0f ac 04 01 00 00 0f ac 02 00

IEEE 802.11 Radiotap Capture ... Packets: 1000 · Dis... Profile: Default

Спасибо за внимание, ваши вопросы