

## Отчет по практическому заданию 1.

### Ход работы.

1. Сначала были установлены VirtualBox ( Windows hosts и VirtualBox 7.1.6 Extension Pack) и Wireshark. Был запущен Wireshark, настроено расположение информационных фреймов и запущен захват пакетов беспроводной сети (рис. 1).

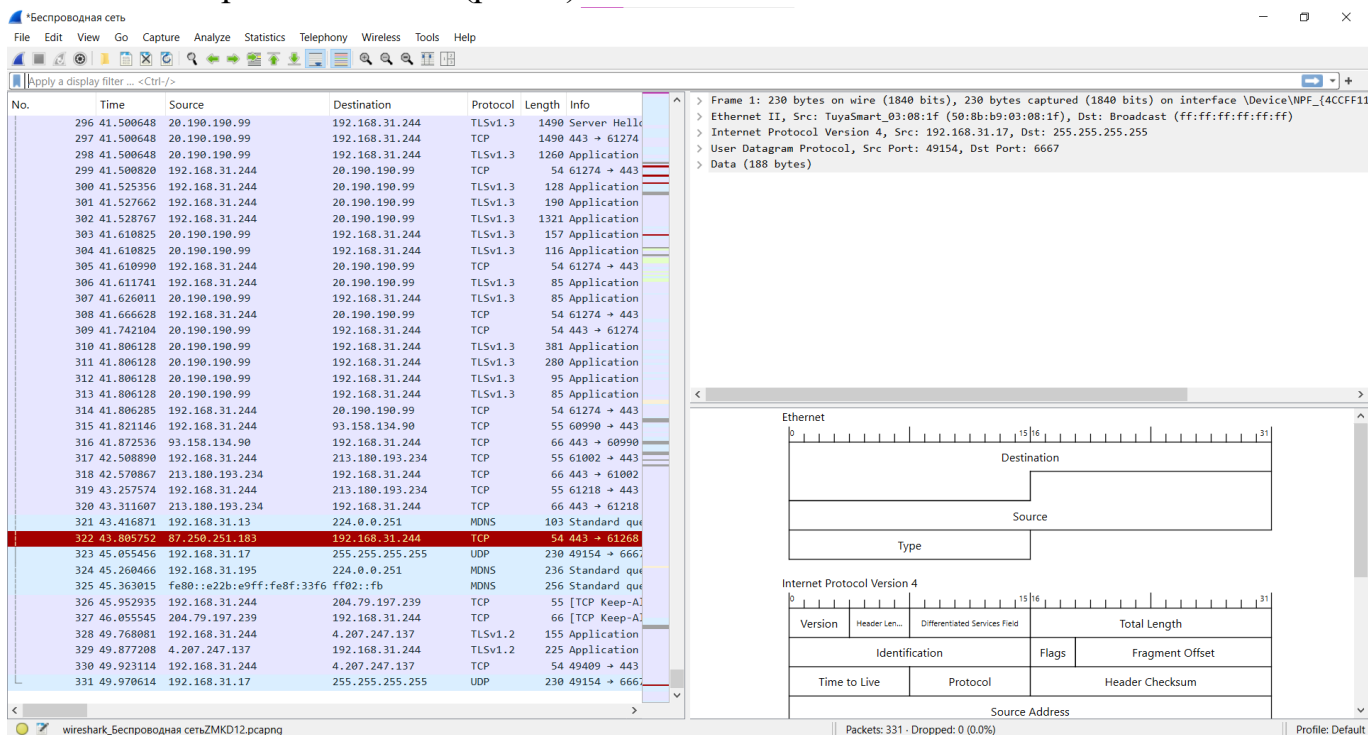


Рис. 1 – захват пакетов беспроводной сети

Наблюдаемая мною информация напрямую связана с моделью OSI/ISO, так как каждый пакет содержит информацию, относящуюся к разным уровням модели OSI (например, сетевой уровень – видны IP-адреса отправителя и получателя).

2. Далее среди захваченных пакетов были найдены пакеты протокола DNS с помощью фильтров (рис. 2)

| dns |           |                |                |          |        |                         |
|-----|-----------|----------------|----------------|----------|--------|-------------------------|
| No. | Time      | Source         | Destination    | Protocol | Length | Info                    |
| 22  | 11.432895 | 192.168.31.244 | 192.168.31.1   | DNS      | 92     | Standard query          |
| 25  | 11.440403 | 192.168.31.1   | 192.168.31.244 | DNS      | 174    | Standard query response |
| 56  | 12.685434 | 192.168.31.244 | 192.168.31.1   | DNS      | 92     | Standard query          |
| 60  | 12.706060 | 192.168.31.1   | 192.168.31.244 | DNS      | 174    | Standard query response |
| 70  | 14.015890 | 192.168.31.244 | 192.168.31.1   | DNS      | 76     | Standard query          |
| 71  | 14.016132 | 192.168.31.244 | 192.168.31.1   | DNS      | 76     | Standard query          |
| 72  | 14.018134 | 192.168.31.1   | 192.168.31.244 | DNS      | 92     | Standard query          |
| 73  | 14.023297 | 192.168.31.244 | 77.88.8.8      | DNS      | 74     | Standard query          |
| 74  | 14.023698 | 192.168.31.244 | 77.88.8.8      | DNS      | 74     | Standard query          |

Рис. 2 – все захваченные пакеты протокола DNS

- Затем я сохранила захваченные пакеты в файл. С помощью командной строки и редактор `editcap` я отредактировала файл так, чтобы в нем осталось только 10 пакетов (рис. 3).

| No. | Time     | Source         | Destination    | Protocol | Length | Info              |
|-----|----------|----------------|----------------|----------|--------|-------------------|
| 1   | 0.000000 | 204.79.197.239 | 192.168.31.244 | TCP      | 54     | 443 → 63703 [RST, |
| 2   | 0.253389 | 98.64.238.3    | 192.168.31.244 | TLSv1.2  | 100    | Application Data  |
| 3   | 0.253389 | 98.64.238.3    | 192.168.31.244 | TLSv1.2  | 85     | Encrypted Alert   |
| 4   | 0.253732 | 192.168.31.244 | 98.64.238.3    | TCP      | 54     | 63699 → 443 [ACK] |
| 5   | 0.253821 | 192.168.31.244 | 98.64.238.3    | TCP      | 54     | 63699 → 443 [FIN, |
| 6   | 0.351981 | 98.64.238.3    | 192.168.31.244 | TCP      | 54     | 443 → 63699 [ACK] |
| 7   | 2.752952 | 192.168.31.244 | 149.154.167.51 | SSL      | 271    | Continuation Data |
| 8   | 2.841975 | 149.154.167.51 | 192.168.31.244 | TCP      | 54     | 443 → 61981 [ACK] |
| 9   | 2.842990 | 149.154.167.51 | 192.168.31.244 | SSL      | 610    | Continuation Data |
| 10  | 2.844013 | 192.168.31.244 | 149.154.167.51 | SSL      | 415    | Continuation Data |

Рис. 3 – файл, отредактированный через `editcap`

- Далее я снова запустила захват с настройкой автоматической остановки захвата после 50 пакетов, а также настроила ширину столбцов по их содержимому (рис. 4 и 5). На этом работа с Wireshark пока окончена.

Автоматически останавливать захват после... —

☒ 50 пакета (пакетов)

Рис. 4 – настройки захвата

| No. | Time     | Source                    | Destination     | Protocol | Length | Info            |
|-----|----------|---------------------------|-----------------|----------|--------|-----------------|
| 1   | 0.000000 | 192.168.31.13             | 239.255.255.250 | SSDP     | 167    | M-SEARCH * HTTP |
| 2   | 0.614234 | 192.168.31.17             | 255.255.255.255 | UDP      | 230    | 49154 → 6667 Le |
| 3   | 1.014708 | 192.168.31.244            | 162.254.198.69  | TLSv1.2  | 113    | Application Dat |
| 4   | 1.081042 | 162.254.198.69            | 192.168.31.244  | TCP      | 54     | 27022 → 62664 [ |
| 5   | 1.463012 | 192.168.31.244            | 149.154.167.151 | TCP      | 54     | 65389 → 443 [FI |
| 6   | 1.555061 | 149.154.167.151           | 192.168.31.244  | TCP      | 54     | 443 → 65389 [FI |
| 7   | 1.555175 | 192.168.31.244            | 149.154.167.151 | TCP      | 54     | 65389 → 443 [AC |
| 8   | 2.560960 | 192.168.31.195            | 224.0.0.251     | MDNS     | 703    | Standard query  |
| 9   | 2.663157 | fe80::e22b:e9ff:fe8f:33f6 | ff02::fb        | MDNS     | 723    | Standard query  |
| 10  | 3.066218 | 192.168.31.244            | 108.177.14.188  | TCP      | 55     | 63694 → 5228 [A |

Рис. 5 – установленная ширины столбцов по содержимому

- Далее требовалось создать виртуальную машину в VirtualBox. Ее нужно было подключить к RouterOSv7, поэтому на шаге выбора объема памяти жесткого диска я выбрала файл с расширением `.vdi`, скачанный с методички. Зарегистрировалась в системе и прочитала лицензию.
- Затем с помощью консоли я изменила имя узла на `mt-00` и режим выключения экрана после бездействия (рис. 6).

```

[admin@mt-00] /console> /system/console/screen
[admin@mt-00] /system/console/screen> set blank-interval=60m
[admin@mt-00] /system/console/screen> print
    line-count: 25
    blank-interval: 60min
[admin@mt-00] /system/console/screen> _

```

Рис. 6 – команды для настройки режима выключения экрана после бездействия

7. После я установила информационное сообщение, выводимое в терминал перед и после запроса авторизационных данных (рис. 7)

```

Bakhireva Alena Andreevna, IS-342
MikroTik 7.16.2 (stable)
mt-00 Login: S_

Press F1 for help

Bakhireva Alena Andreevna, IS-342

```

Рис. 7 – информационное сообщение

8. Далее вывела информацию о пользовательских группах (рис.8)

```

[admin@mt-00] > /user print
Columns: NAME, GROUP, LAST-LOGGED-IN, INACTIVITY-POLICY
# NAME  GROUP  LAST-LOGGED-IN  INACTIVITY-POLICY
;;; system default user
0 admin full  2025-02-07 03:16:36  none
[admin@mt-00] > /user group print
0 name="read" policy=local,telnet,ssh,reboot,read,test,winbox,password,web,
  sniff,sensitive,api,romon,rest-api,!ftp,!write,!policy
  skin=default

1 name="write" policy=local,telnet,ssh,reboot,read,write,test,winbox,password,
  web,sniff,sensitive,api,romon,rest-api,!ftp,!policy
  skin=default

2 name="full" policy=local,telnet,ssh,ftp,reboot,read,write,policy,test,winbox,
  password,web,sniff,sensitive,api,romon,rest-api
  skin=default
[admin@mt-00] > _

```

Рис. 8 – информация о пользователях

В MikroTik policy - набору правил или настроек, которые определяют доступ и права пользователей, а также управление трафиком и ресурсами устройства.

9. Затем я остановила и создала вторую виртуальную машину на базе того же виртуального диска. Потом снова запустила 2 машины (рис. 9)

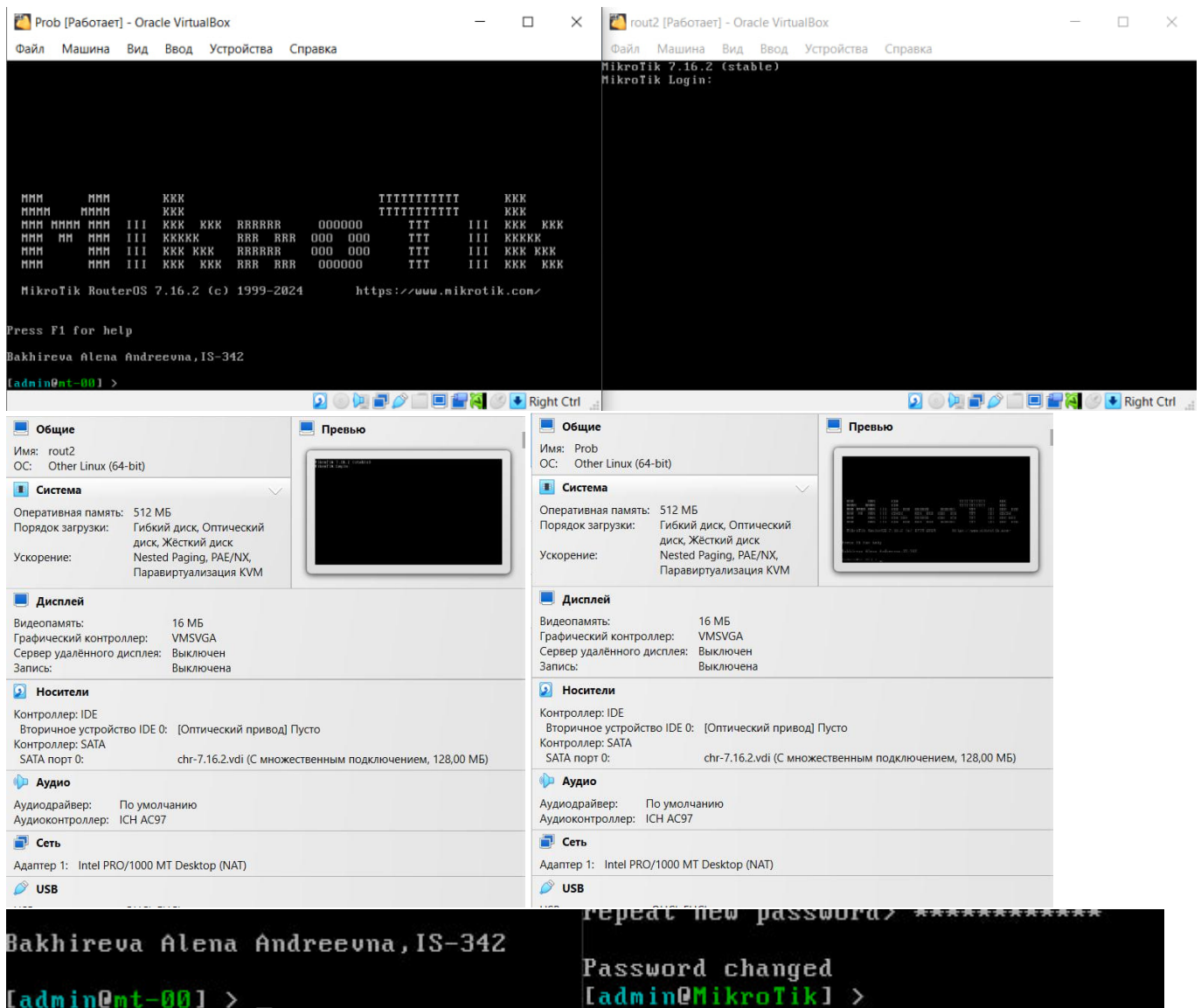


Рис. 9 – различие настроек двух виртуальных машин

Дальше я клонировала изначальную виртуальную машину и сравнивала ее с созданной на базе того же виртуального диска. Отличие заключалось в том, что клонированная машина имела настройки машины, с которой ее клонировали, а созданная на базе диска имела настройки по умолчанию.

10. Затем я просто экспортировала конфигурации, удалила машину и импортировала конфигурации. На этом работа с RouterOSv7 и Mikrotik пока окончена
11. Далее я создала новую виртуальную машину с образом БазальтОС и с помощью Менеджера виртуальных носителей переключила жесткий виртуальный диск в режим множественного использования.
12. Зайдя в систему под учетной записью администратора, с помощью команды `journalctl -t network` вывела записи от источника с идентификатором network (рис. 10)



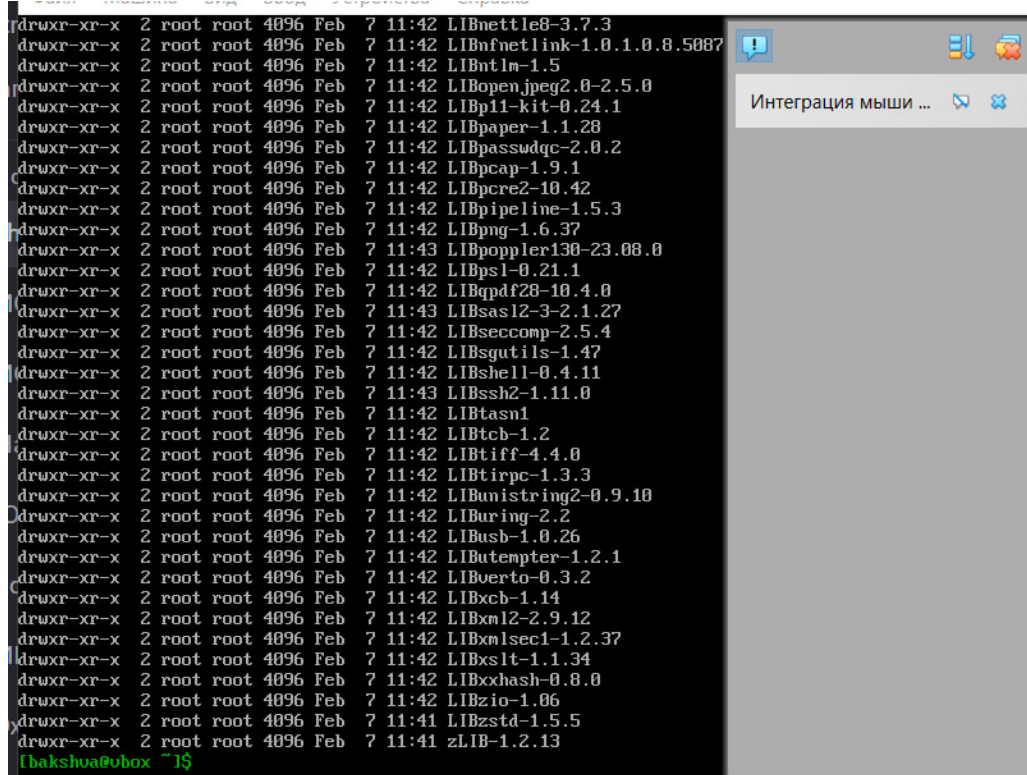
```

[root@vbox ~]# journalctl -t network
Feb 07 11:58:57 vbox network[2469]: Computing interface groups: .. 2 interfaces found
Feb 07 11:58:57 vbox network[2469]: Starting group 0/virtual (1 interfaces)
Feb 07 11:58:57 vbox network[2469]: Starting lo:
Feb 07 11:58:57 vbox network[2504]: 'lo' is already up
Feb 07 11:58:57 vbox network[2469]: SKIPPED
Feb 07 11:58:58 vbox network[2469]: Starting group 1/realphys (1 interfaces)
Feb 07 11:58:58 vbox network[2469]: Starting enp0s3:
Feb 07 11:58:58 vbox network[2523]: .
Feb 07 11:58:58 vbox network[2535]: .
Feb 07 11:58:58 vbox network[2537]: .
Feb 07 11:58:58 vbox network[2545]: dhcpcd-10.0.6 starting
Feb 07 11:58:58 vbox network[2548]: enp0s3: waiting for carrier
Feb 07 11:59:00 vbox network[2548]: enp0s3: carrier acquired
Feb 07 11:59:01 vbox network[2548]: enp0s3: soliciting a DHCP lease
Feb 07 11:59:01 vbox network[2548]: enp0s3: offered 10.0.2.15 from 10.0.2.2
Feb 07 11:59:01 vbox network[2548]: enp0s3: leased 10.0.2.15 for 86400 seconds
Feb 07 11:59:01 vbox network[2548]: enp0s3: adding route to 10.0.2.0/24
Feb 07 11:59:01 vbox network[2548]: enp0s3: adding default route via 10.0.2.2
Feb 07 11:59:02 vbox network[2537]: .
Feb 07 11:59:02 vbox network[2535]: .
Feb 07 11:59:02 vbox network[2469]: OK
Feb 07 11:59:02 vbox network[2469]: Processing /etc/net/vlantab: empty.

```

Рис. 10 – вывод записей от источника с идентификатором network

13. Далее я перешла в профиль пользователя, созданный при установке Базальт ОС, и вывела на экран полную информацию об элементах каталога /usr/share/doc, в именах которых есть три буквы lib и изменив выводимые имена таким образом, чтобы указанные три буквы имели верхний регистр (рис. 13).



```

drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBnettle8-3.7.3
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBnftlink-1.0.1.0.8.5087
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBntlm-1.5
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBopenjpeg2.0-2.5.0
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBp11-kit-0.24.1
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBpaper-1.1.28
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBpasswdqc-2.0.2
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBpcap-1.9.1
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBpcre2-10.42
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBpipeline-1.5.3
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBpng-1.6.37
drwxr-xr-x 2 root root 4096 Feb 7 11:43 LIBpoppler130-23.08.0
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBpsl-0.21.1
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBqpdf28-10.4.0
drwxr-xr-x 2 root root 4096 Feb 7 11:43 LIBsass12-3-2.1.27
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBseccomp-2.5.4
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBsgutils-1.47
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBshell-0.4.11
drwxr-xr-x 2 root root 4096 Feb 7 11:43 LIBssh2-1.11.0
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBtasn1
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBtcb-1.2
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBtiff-4.4.0
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBtirpc-1.3.3
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBunistring2-0.9.10
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBuring-2.2
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBusb-1.0.26
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIButempter-1.2.1
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBuutils-0.3.2
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBxcb-1.14
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBxml2-2.9.12
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBxmlsec1-1.2.37
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBxslt-1.1.34
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBxxhash-0.8.0
drwxr-xr-x 2 root root 4096 Feb 7 11:42 LIBzio-1.06
drwxr-xr-x 2 root root 4096 Feb 7 11:41 LIBzstd-1.5.5
drwxr-xr-x 2 root root 4096 Feb 7 11:41 zLIB-1.2.13

```

Рис. 13 – элементы каталога с lib

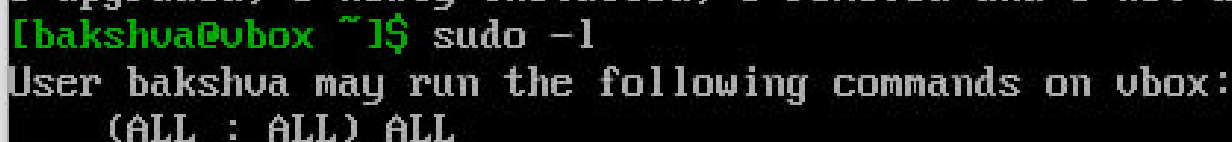
14. Затем с помощью vim я написала скрипт BASH, который выводит параметры строки запуска скрипта с указанием их порядкового номера в командной строке (рис. 14).



```
[root@vbox ~]# ./script.sh раз два три
Параметр 1: раз
Параметр 2: два
Параметр 3: три
```

Рис. 14 – пример работы скрипта

15. Далее я помощью потокового редактора sed, удалила в файле /etc/sudoers символы ”# “ в начале строк содержащих подстроку SUDO\_USERS (командой `sed -i '/SUDO_USERS/ s/^# //' /etc/sudoers`). Также на этом шаге я добавила группу пользователей sudo и включила в неё локального пользователя (рис. 15)



```
[bakshua@vbox ~]$ sudo -l
User bakshua may run the following commands on vbox:
(ALL : ALL) ALL
```

Рис. 15 – у локального пользователя есть права sudo

На этом работа с БазальтОС пока окончена.

16. Я создала еще одну виртуальную машину, используя образ AstraLinux. Запустила ее, установила операционную систему. Затем я создала в каталоге /etc/network/interfaces.d файл eth0 и с помощью nano добавила в него 2 строки из методички. Убедилась, что установка автоматического получения IP-адреса через DHCP при загрузке системы прошла успешно. После этого я выключила виртуальную машину и через менеджер виртуальных носителей изменила тип виртуального жесткого диска на «с множественным подключением».
17. Далее требовалось вывести информацию о всех пакетах, начинающихся с git. Для этого мне потребовалось обновить список доступных пакетов и их версий (`sudo apt update`), ибо без нее команда поиска не работала. После этого запустила поиск (рис. 16).

```

git-doc/stable,stable,now 1:2.11.0-3+deb9u7 all [установлен, автоматически]
fast, scalable, distributed revision control system (documentation)

git-el/stable,stable,now 1:2.11.0-3+deb9u7 all [установлен, автоматически]
fast, scalable, distributed revision control system (emacs support)

git-email/stable,stable,now 1:2.11.0-3+deb9u7 all [установлен, автоматически]
fast, scalable, distributed revision control system (email add-on)

git-flow/stable 1.10.2-1 all
Git extension to provide a high-level branching model

git-gui/stable,stable,now 1:2.11.0-3+deb9u7 all [установлен, автоматически]
fast, scalable, distributed revision control system (GUI)

git-man/stable,stable,now 1:2.11.0-3+deb9u7 all [установлен, автоматически]
fast, scalable, distributed revision control system (manual pages)

git-mediawiki/stable,stable,now 1:2.11.0-3+deb9u7 all [установлен, автоматически]
fast, scalable, distributed revision control system (MediaWiki remote helper)

git-merge-changelog/stable 20140202+stable-2+deb9u1 amd64
git merge driver for GNU ChangeLog files

git-svn/stable,stable,now 1:2.11.0-3+deb9u7 all [установлен, автоматически]
fast, scalable, distributed revision control system (svn interoperability)

gitk/stable,stable,now 1:2.11.0-3+deb9u7 all [установлен, автоматически]
fast, scalable, distributed revision control system (revision tree visualizer)

gitolite3/stable 3.6.6-1 all
SSH-based gatekeeper for git repositories (version 3)

gitweb/stable,stable,now 1:2.11.0-3+deb9u7 all [установлен, автоматически]
fast, scalable, distributed revision control system (web interface)

```

Рис. 16 – результаты поиска

Затем установила метапакет git-all (sudo apt install git-all).

18. После я создала каталог project и инициализировала в нем локальный git репозиторий, добавила произвольный файл и посмотрела какая ветка создана по умолчанию (рис.17).

```

user@astra:~$ mkdir project
Для вас есть почта в /var/mail/user
user@astra:~$ ls
project
user@astra:~$ cd project/
user@astra:~/project$ git init
Инициализирован пустой репозиторий Git в /home/user/project/.git/

user@astra:~/project$ git branch
* master

```

Рис. 17 – работа с git в AstraLinux

19. На последнем шаге я настроила приглашение командной строки bash таким образом, чтобы при наличии в текущем каталоге локального git

репозитория в командной строки выводилось название текущей рабочей ветки (рис. 18).

```
if [ -f /usr/share/git/completion/git-prompt.sh ]; then
    source /usr/share/git/completion/git-prompt.sh
elif [ -f /etc/bash_completion.d/git-prompt ]; then
    source /etc/bash_completion.d/git-prompt
elif [ -f /usr/local/etc/bash_completion.d/git-prompt ]; then
    source /usr/local/etc/bash_completion.d/git-prompt
fi

export PS1='\u@\h:\w$(__git_ps1 "(%s)")\$'
```

```
user@astra:~/project(master)\source ~/.bashrc
user@astra:~/project(master)$
```

Рис. 18 – изменения в bash и запущенная программа