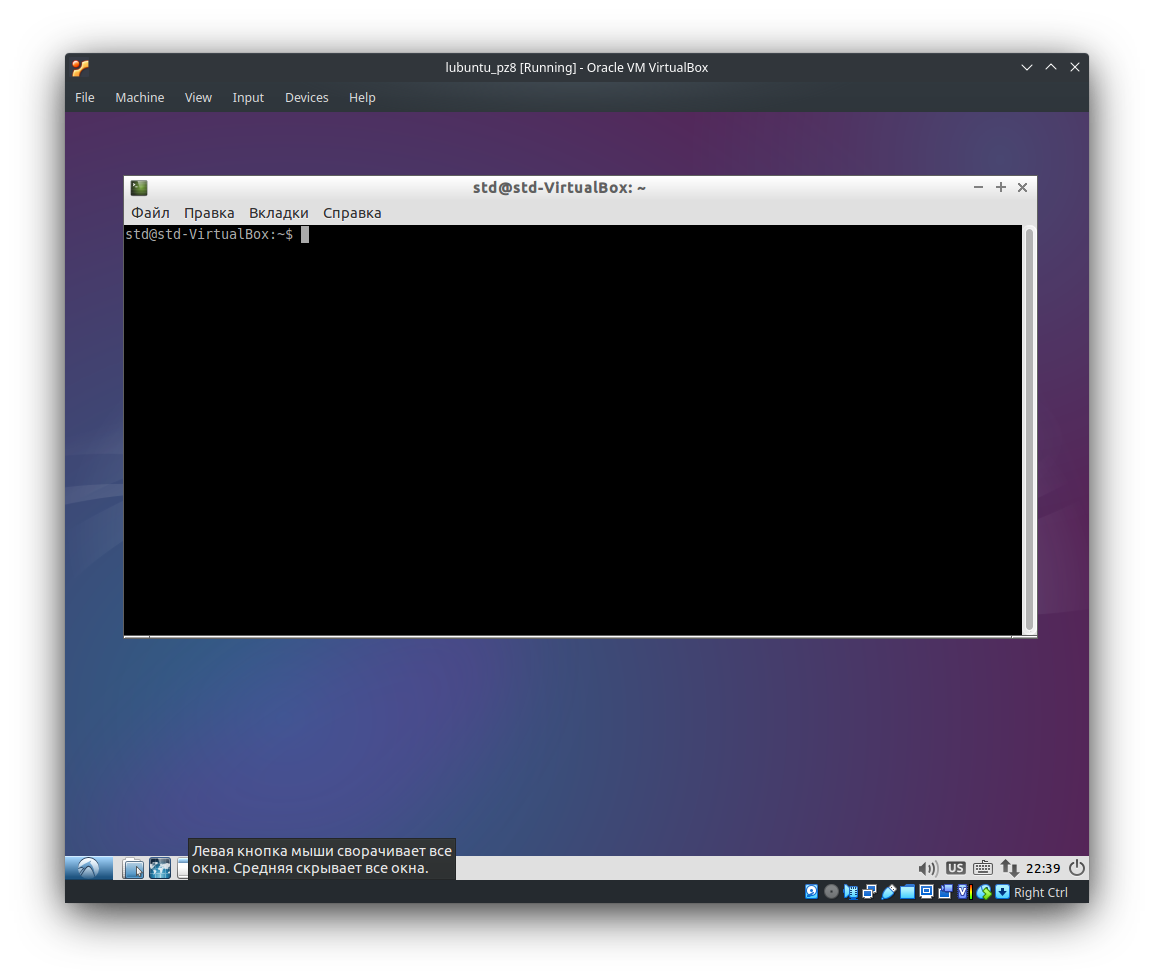
Исследование следов в ОС Linux

**Вопрос 1. Прослеживание загрузки операционной системы .**

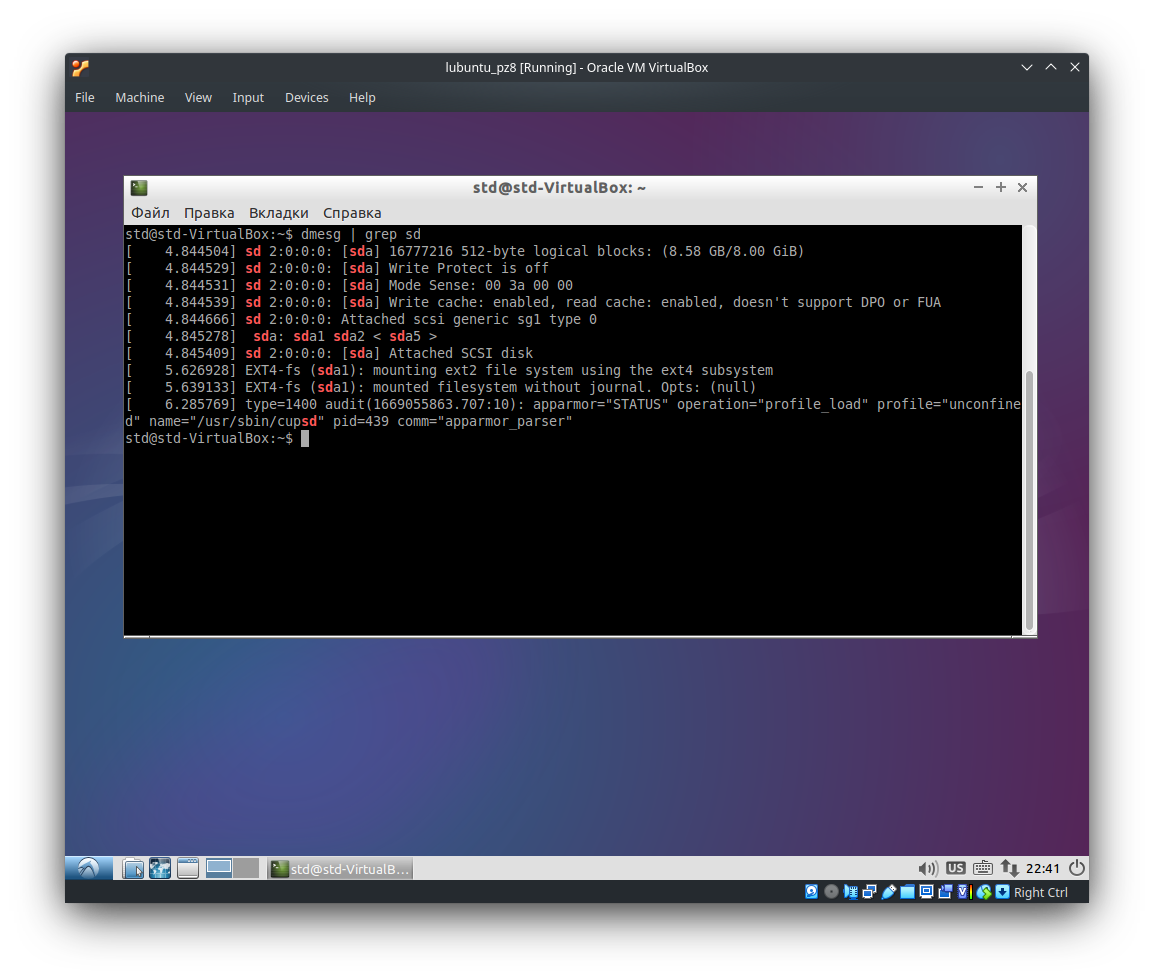
**Задание 1. Прослеживание загрузки операционной системы.**

Зарегистрируемся в системе под пользователем std, используя пароль 123456.



Для выяснения, какие устройства памяти обнаружены в системе, выполним, например, команду

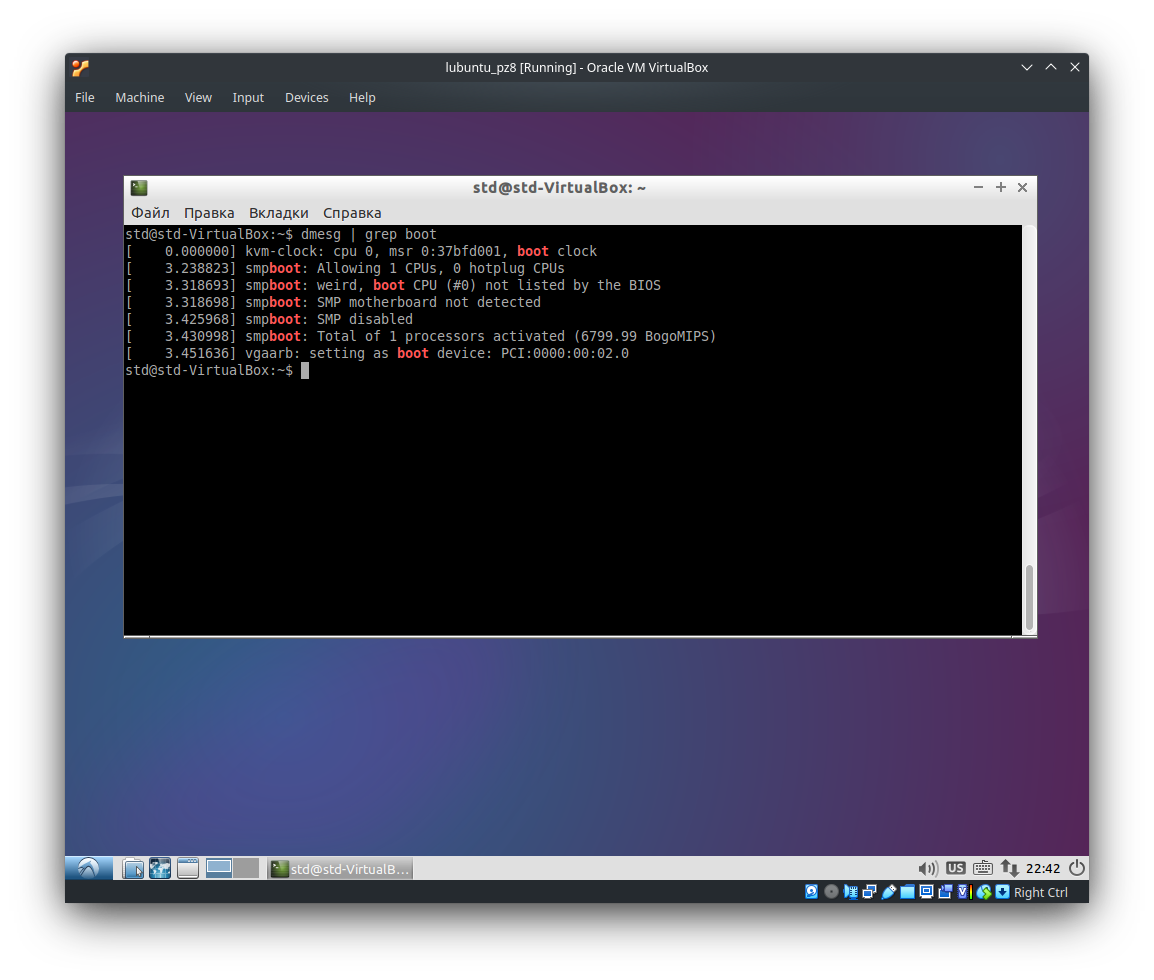
dmesg | grep sd



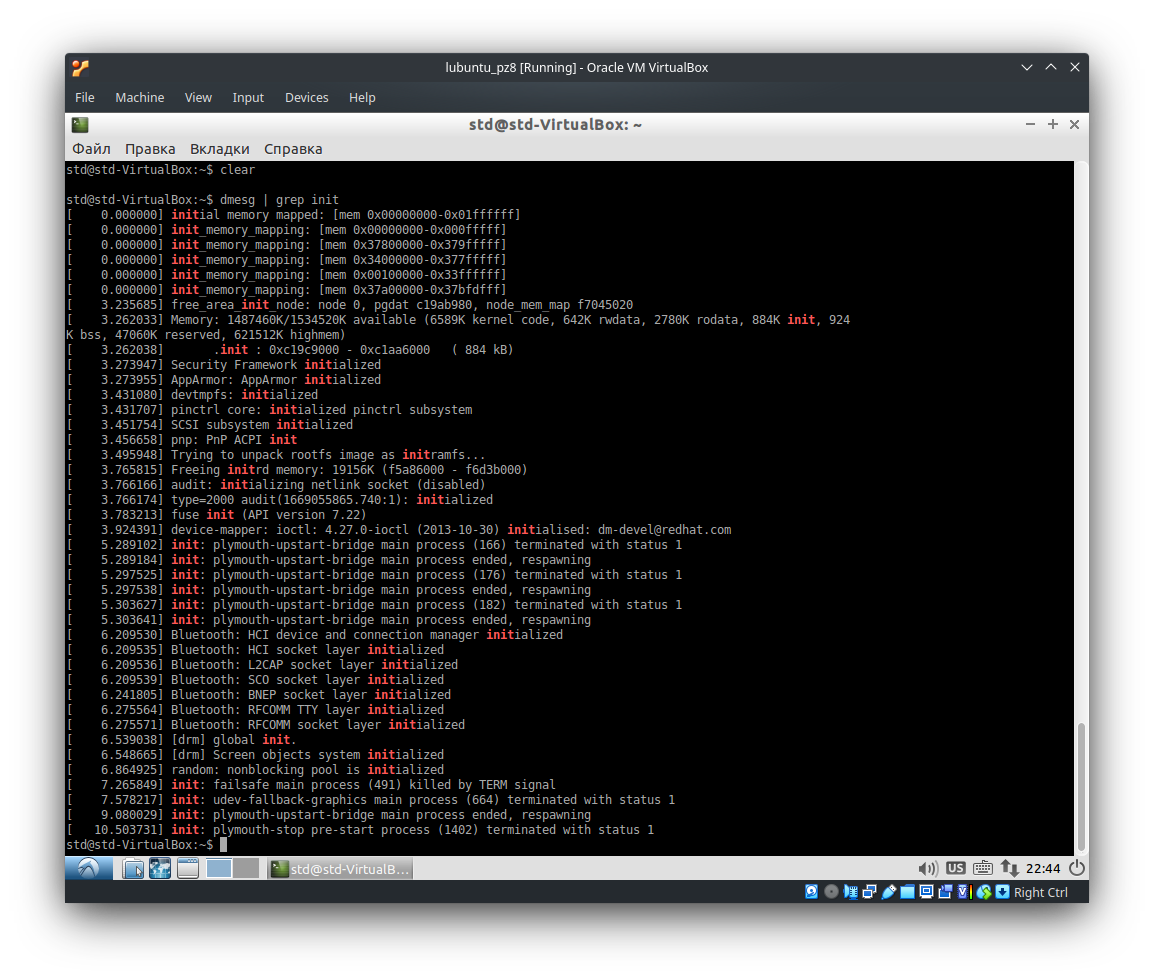
Команда grep выделит только те строки сообщения, в которых присутствует последовательность символов sd.

Придумайте строку, которая покажет информацию о загрузке системы. Укажите ее в отчете и результат ее работы.

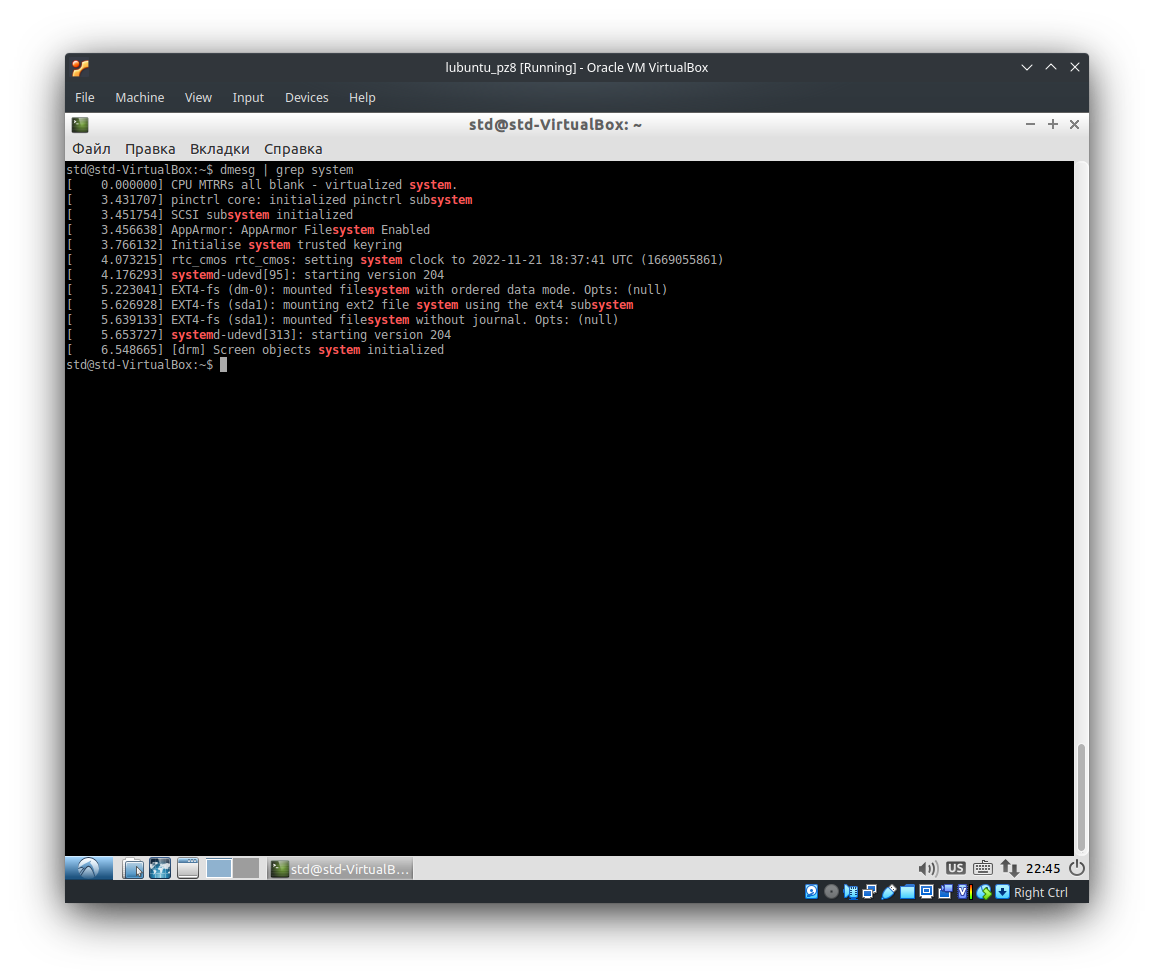
dmesg | grep boot



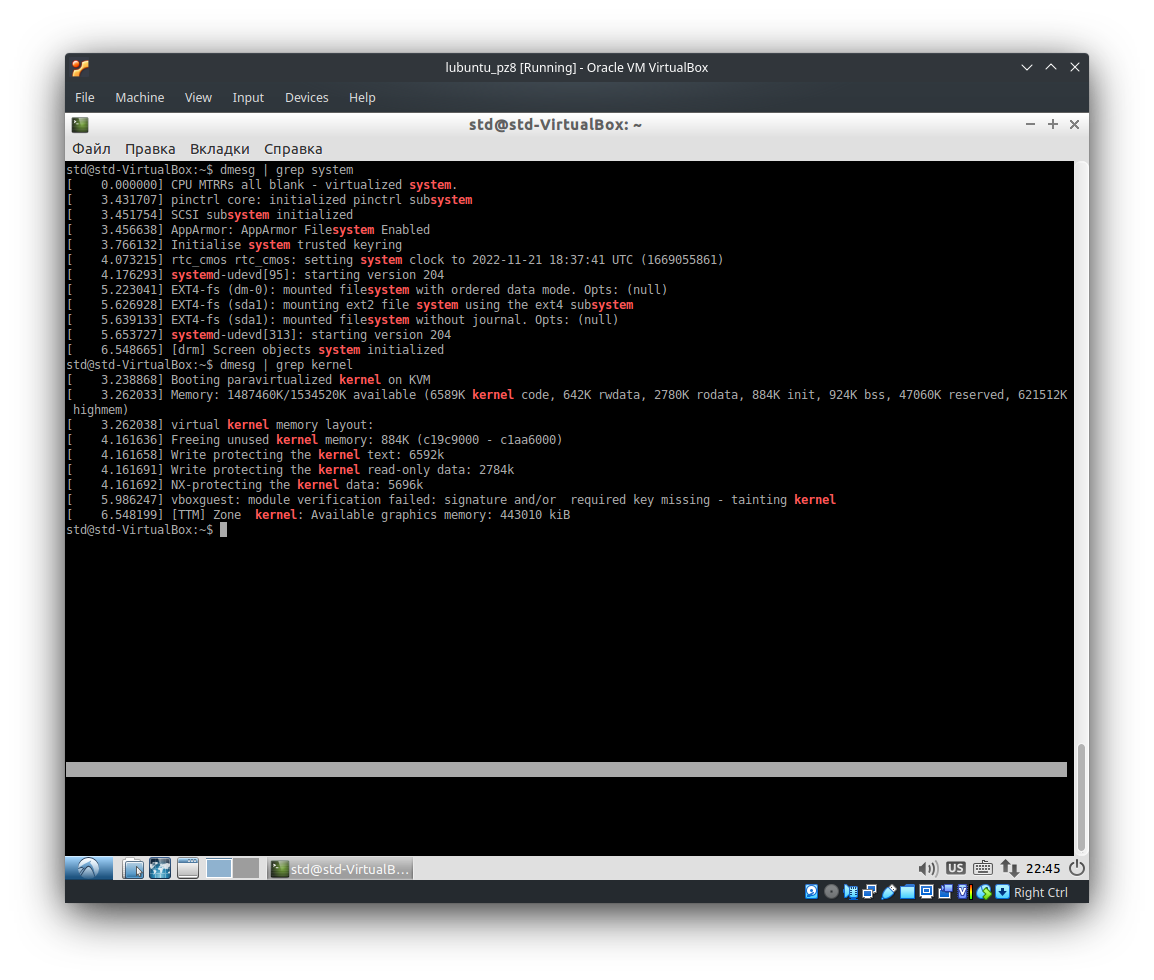
dmesg | grep init



dmesg | grep system



dmesg | grep kernel

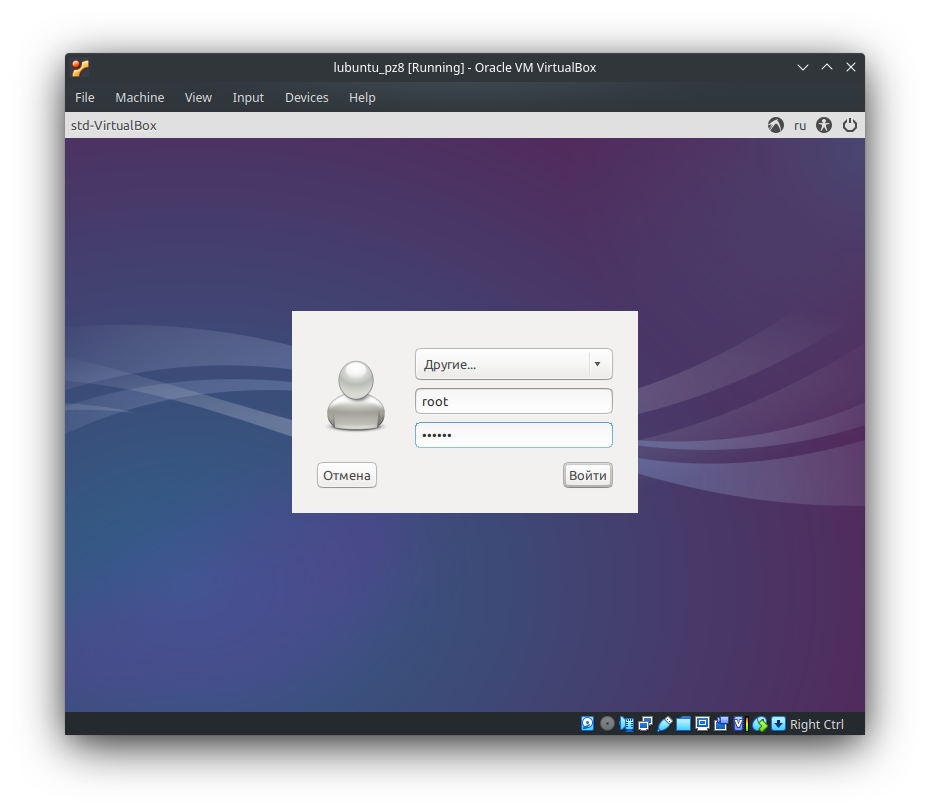


Выйти из системы, завершив сеанс.

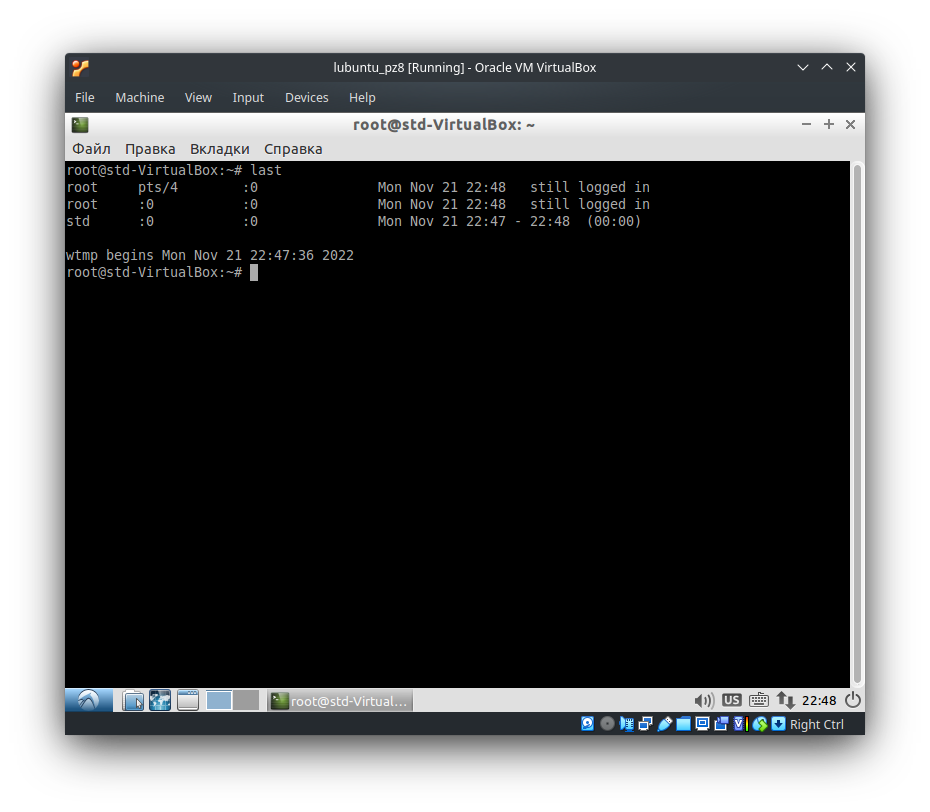
**Задание 2. Определение факта доступа к системе.**

Часто возникает задача установить факт доступа пользователя к системе. Для этого используют команду last. Эта команда обращается к файлу /var/log/wtmp, в котором хранится информация о заходах в систему пользователей.

1) Зарегистрироваться в системе как пользователь root с паролем 123456.



2) Выполнить команду last.



Обратите внимание: сколько раз входил в систему пользователи std и root?

Root - 2 раза (по факту 1), std - 1 раз

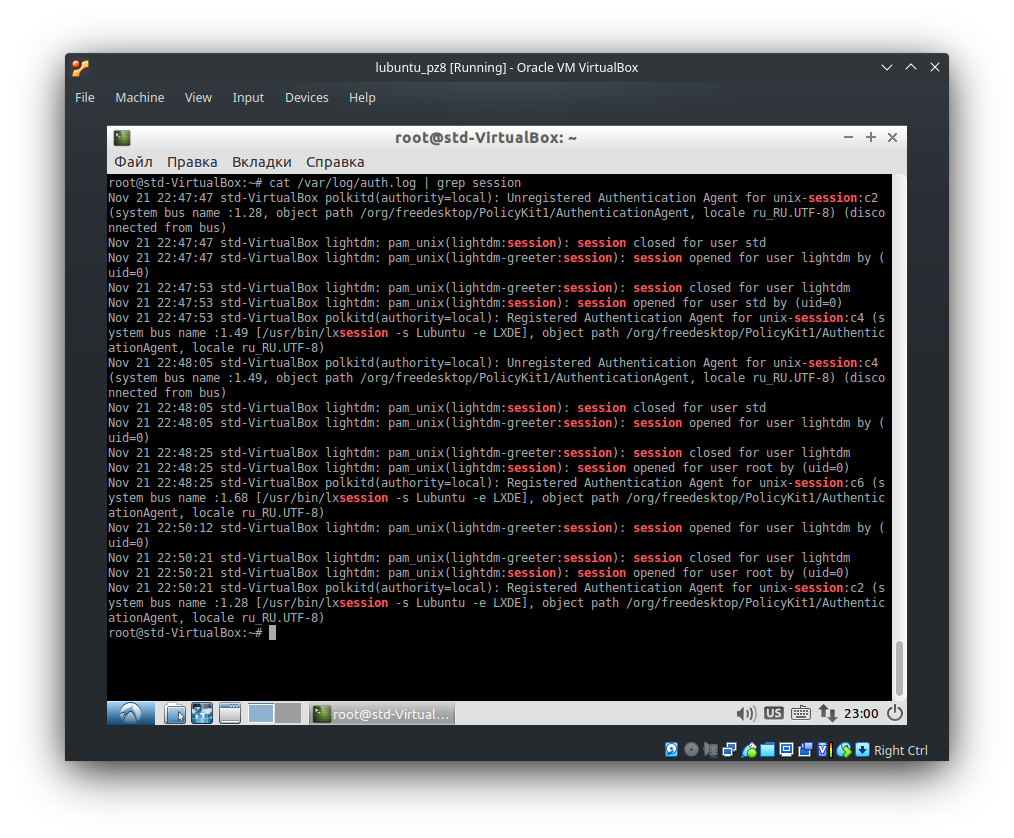
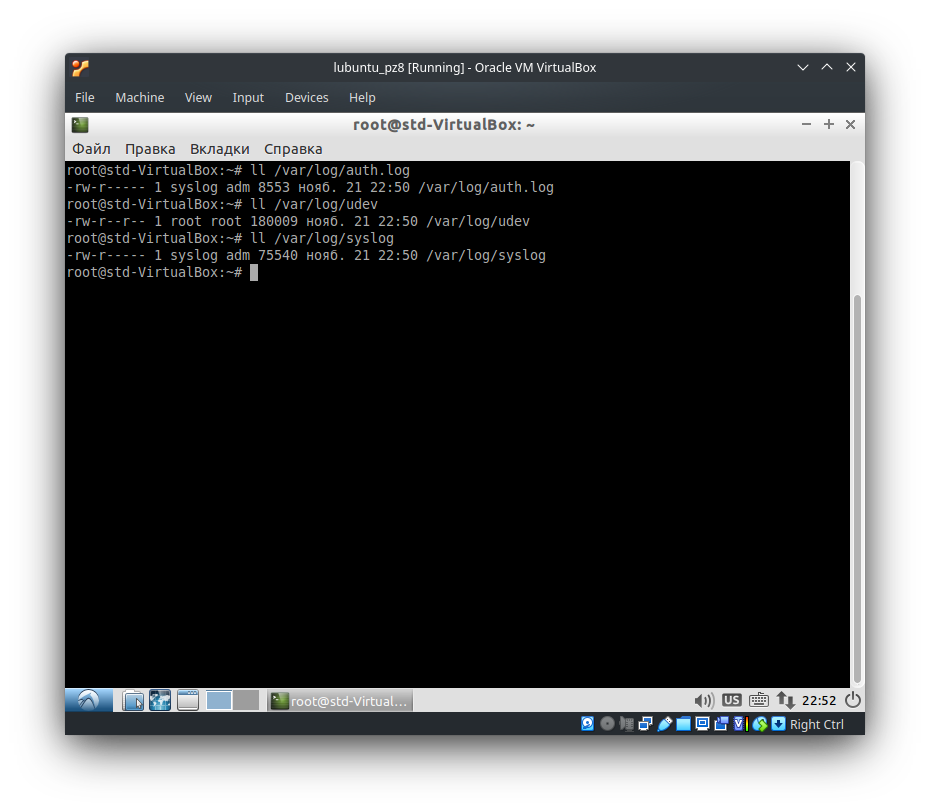
Попробуем перезагрузиться и снова зайти под root



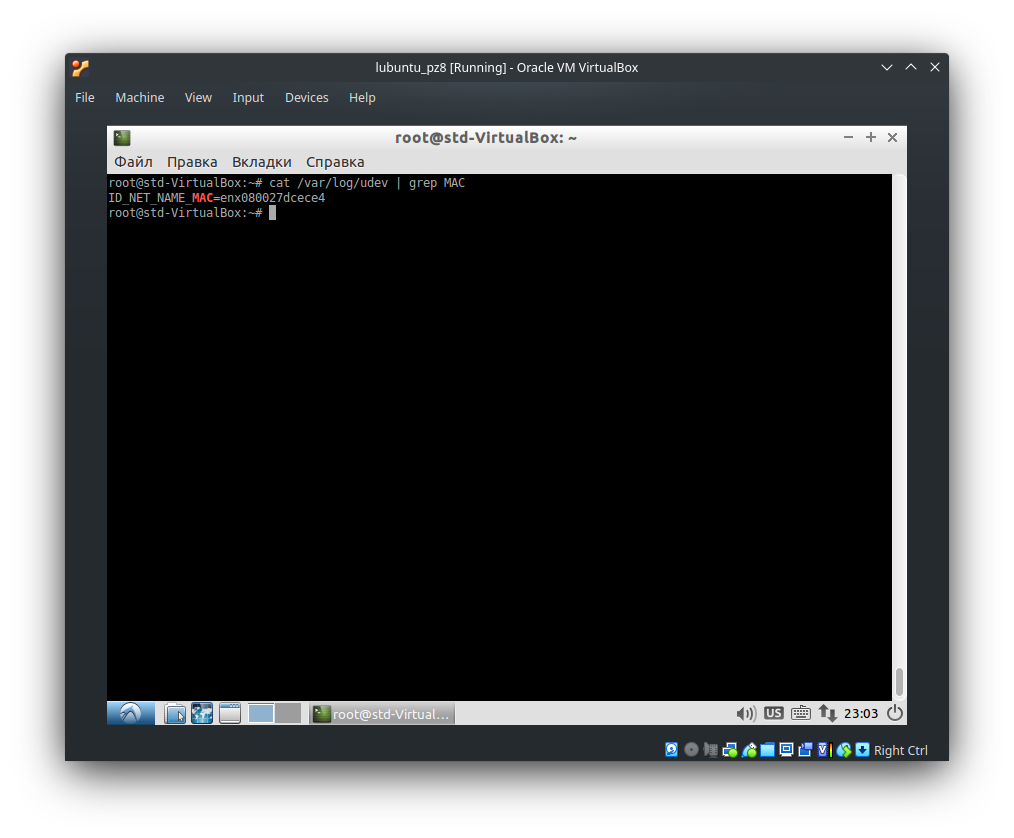
Изменения записей очевидна

**Задание 3. Исследование файлов регистрации /var/log/auth.log, /var/log/udev, /var/log/syslog,**

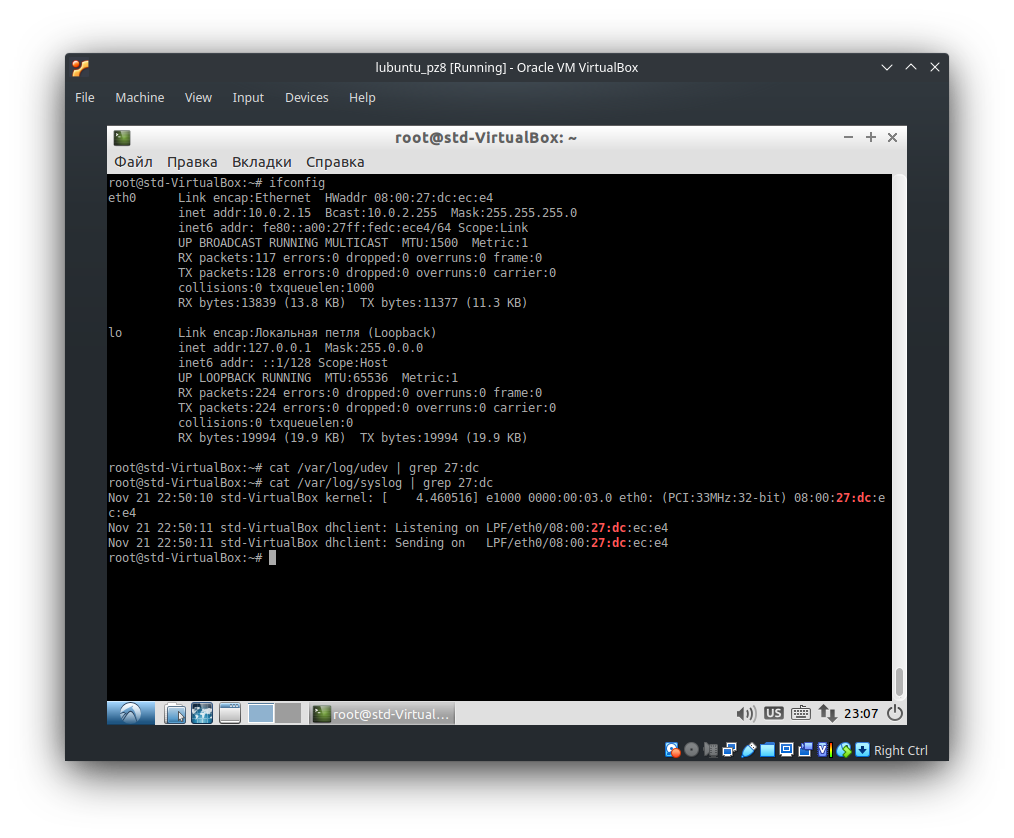
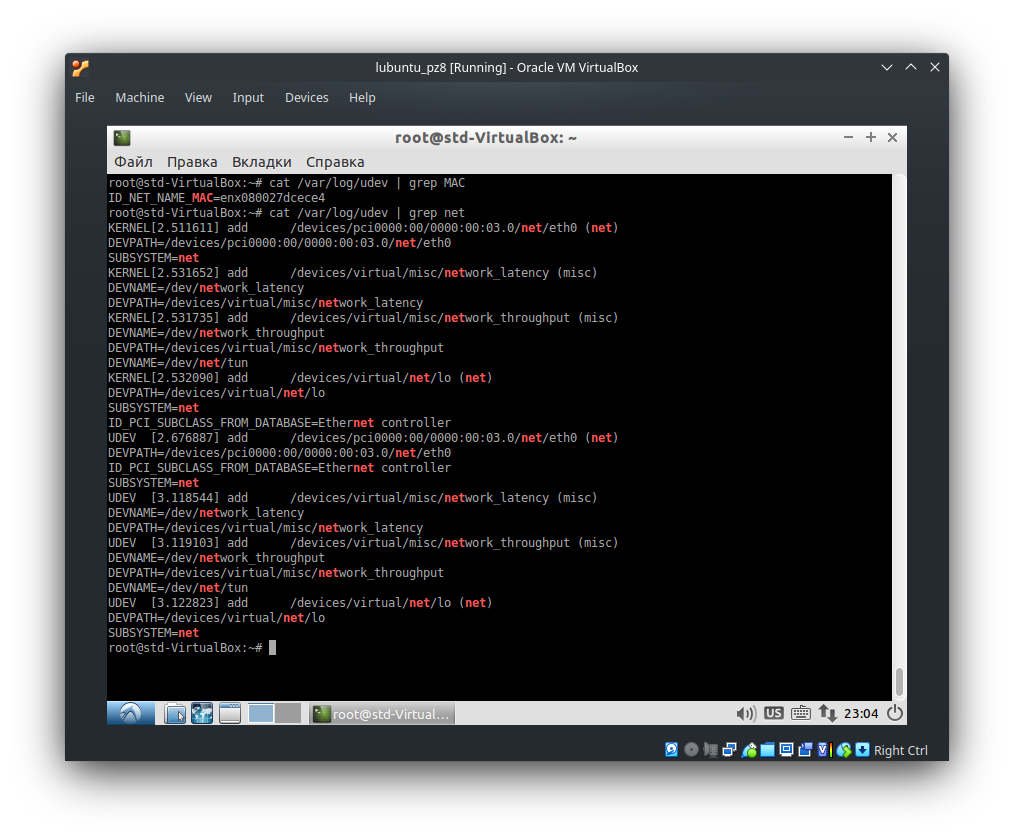
1) Найти в них информацию о регистрации в системе пользователей std и root.



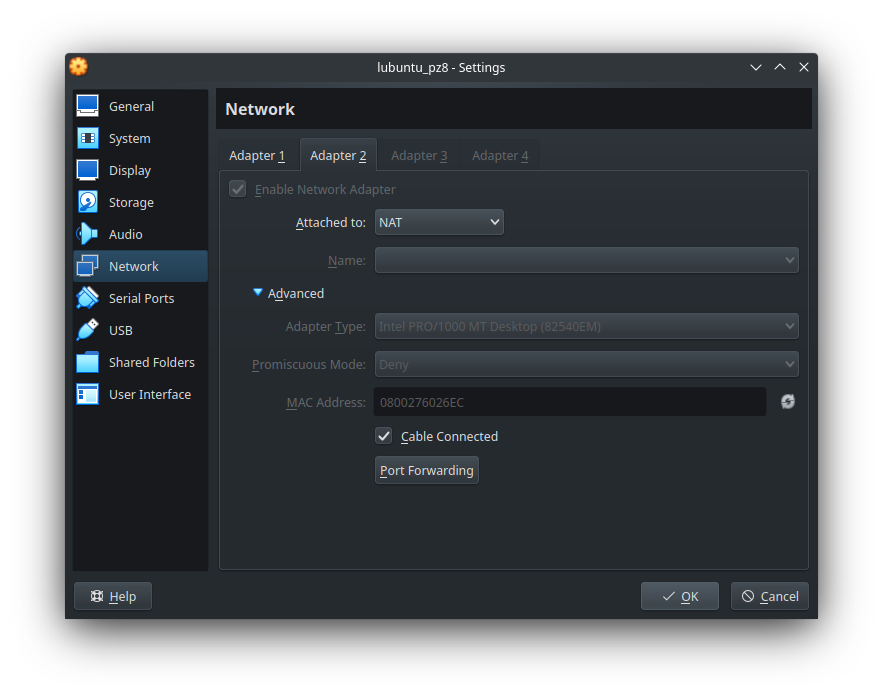
2) Найти сообщения о присвоении машине сетевого IP-адреса. Каково его значение (сообщение от NetworkManager … address)?



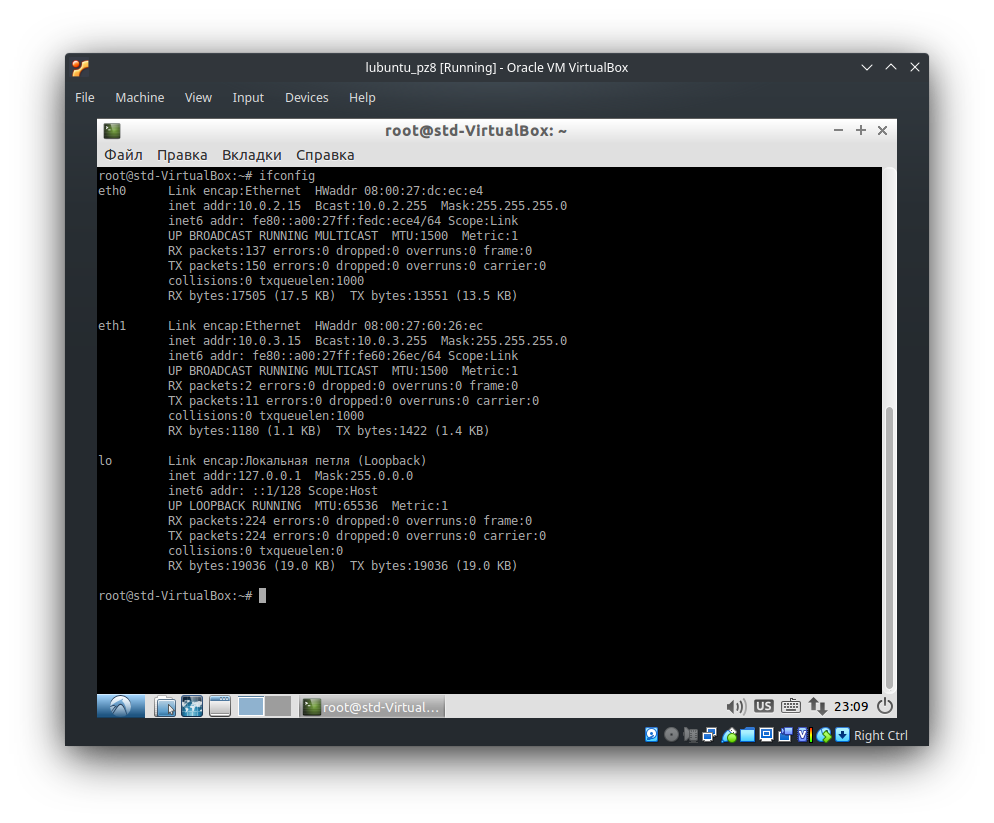
3) Найти сообщения об обнаружении сетевой платы и ее MAC-адрес



Выключите виртуальную машину. Установите еще один виртуальный сетевой адаптер в режиме NAT.



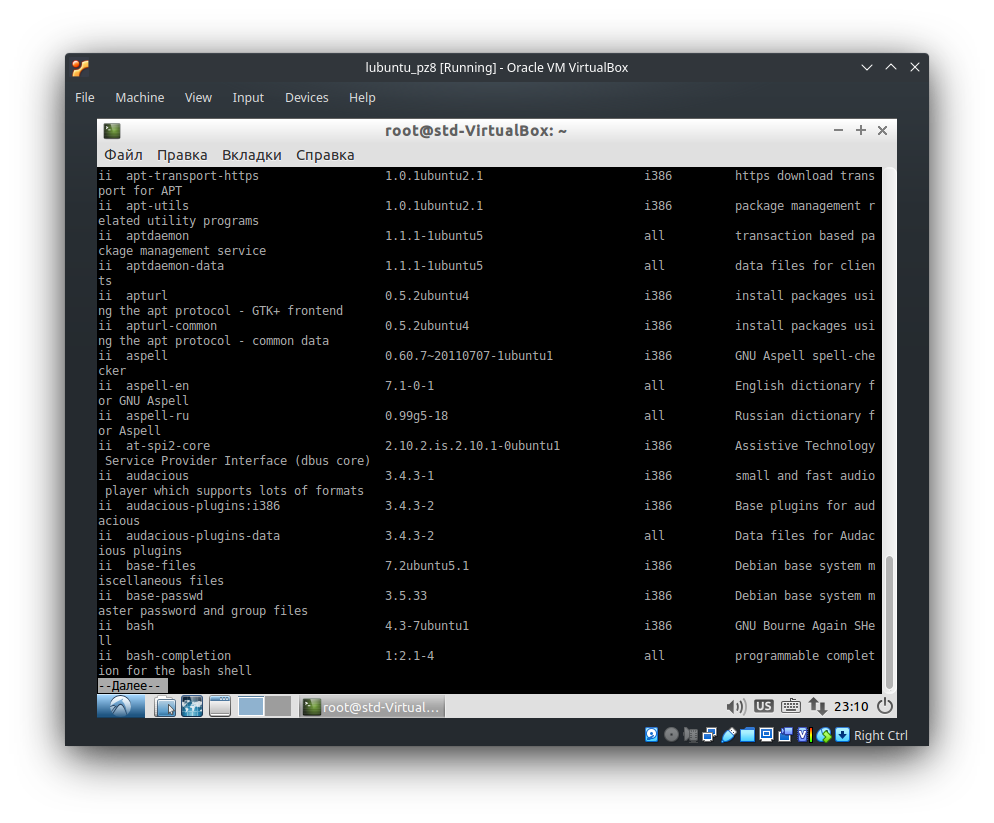
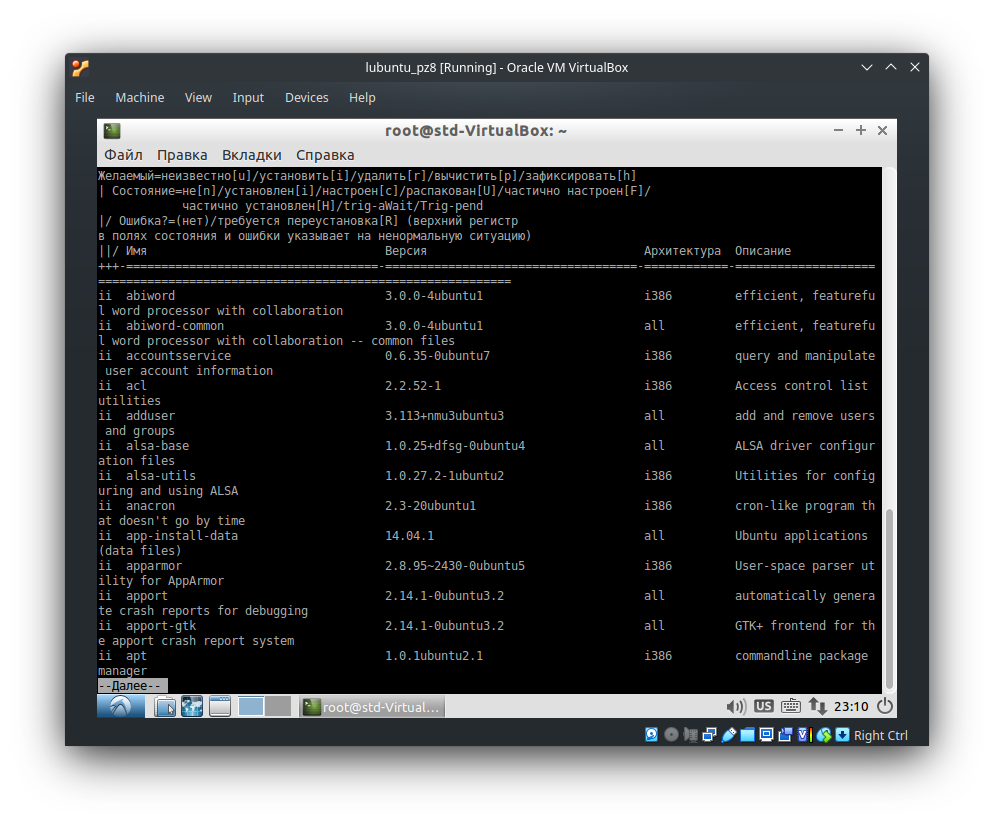
4) Найти адрес сетевого узла, воспринимаемого как возможный маршрутизатор (сообщение от NetworkManager … gateway).



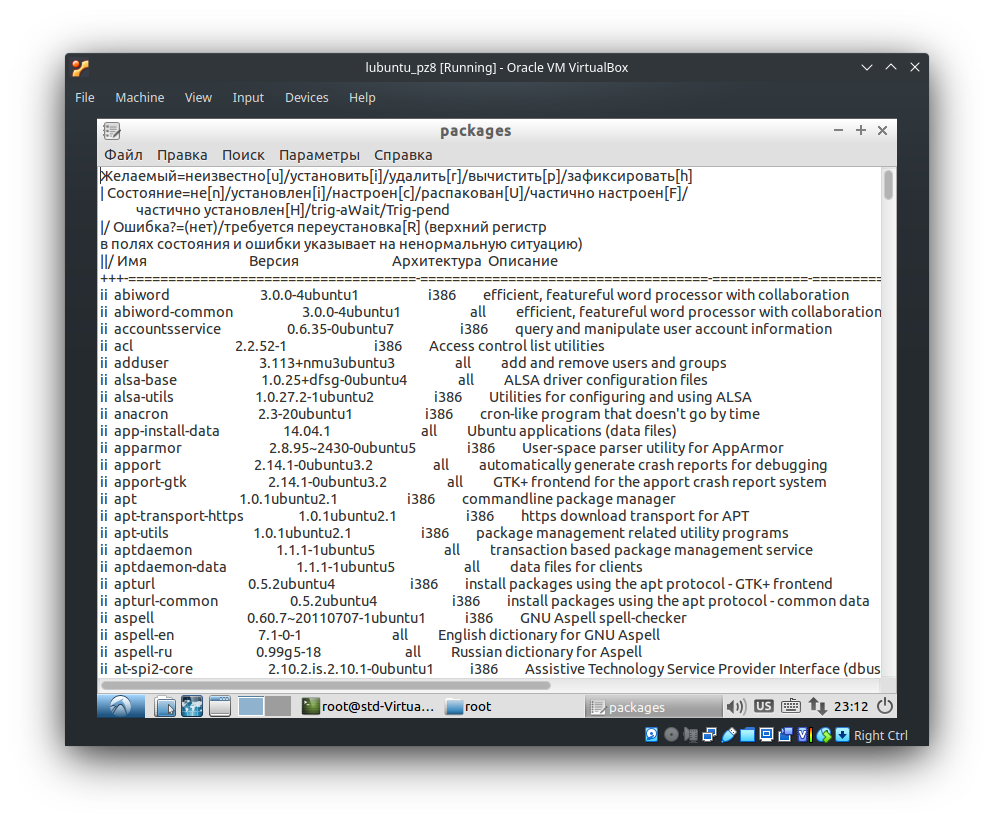
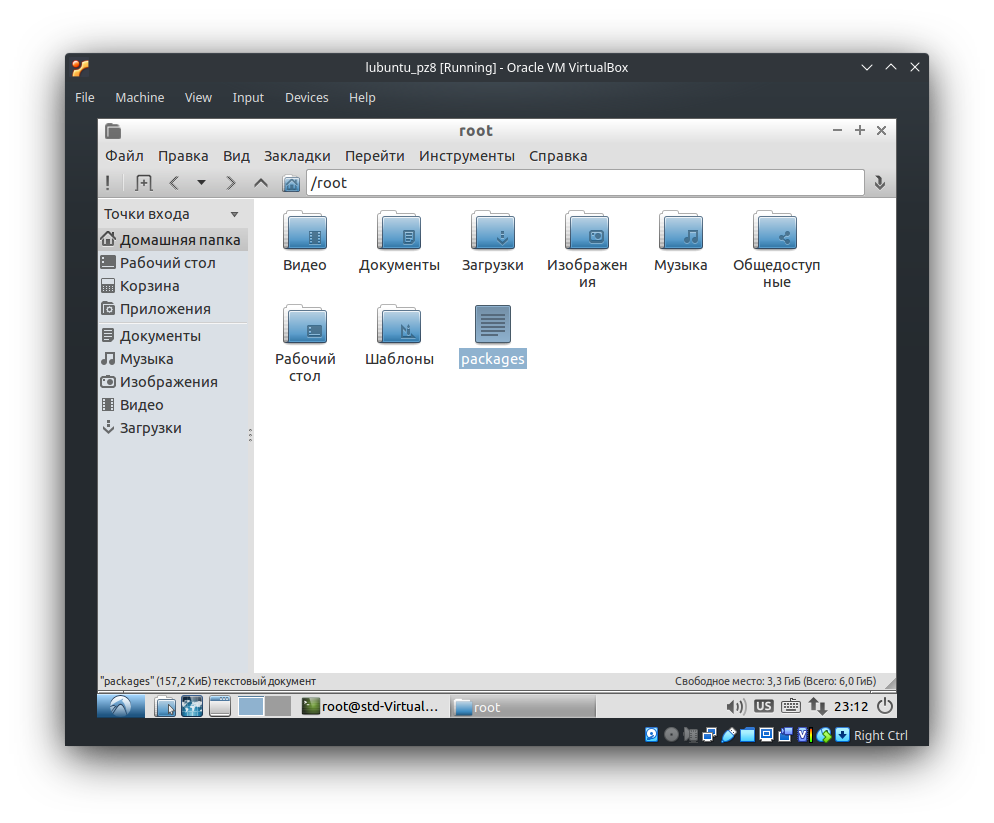
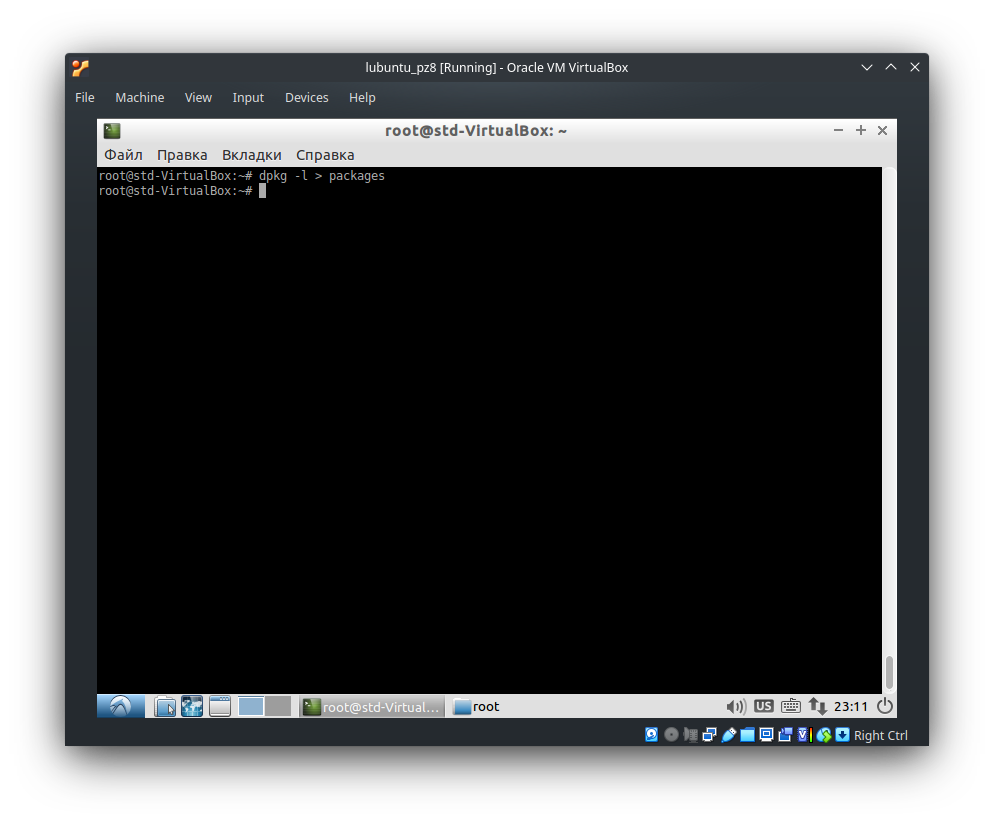
**Задание 4. Определение установленного программного обеспечения**

Для получения информации об установленном программном обеспечении Linux Debian используют команду dpkg

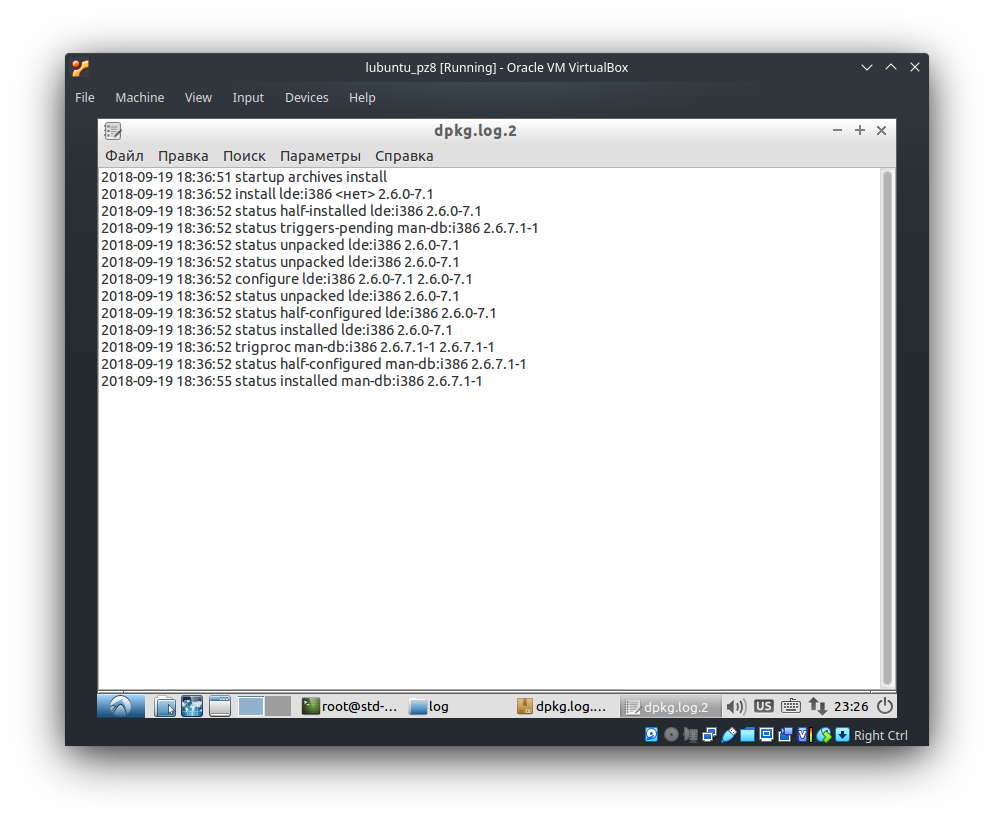
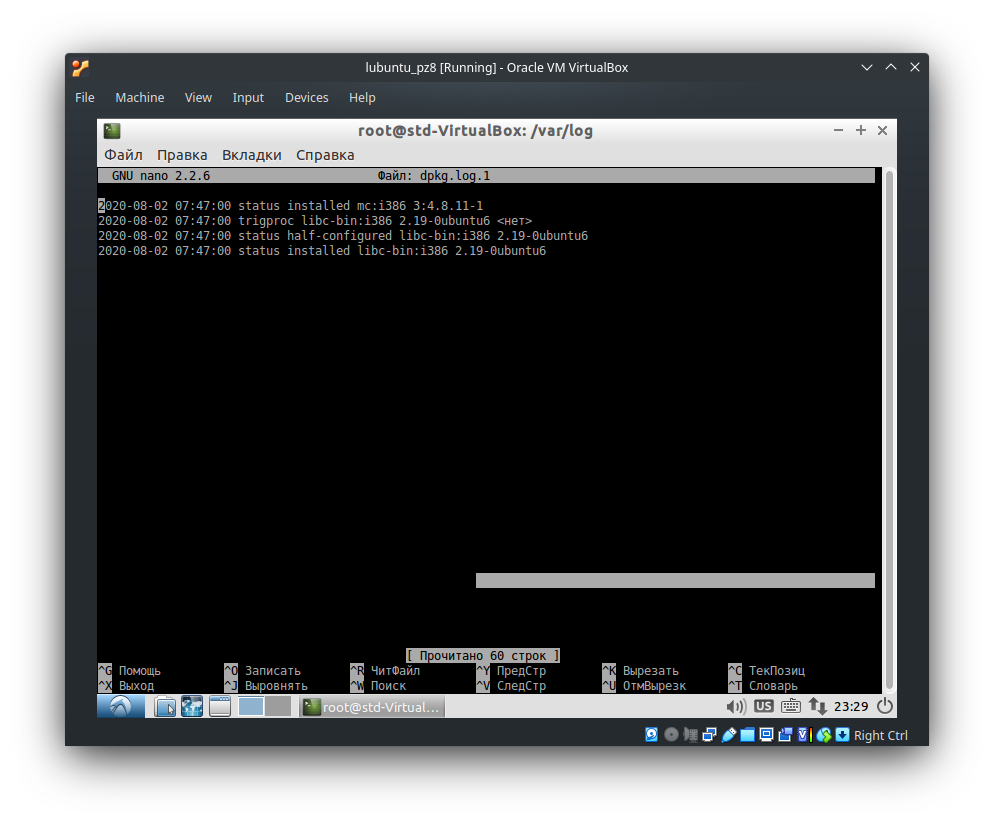
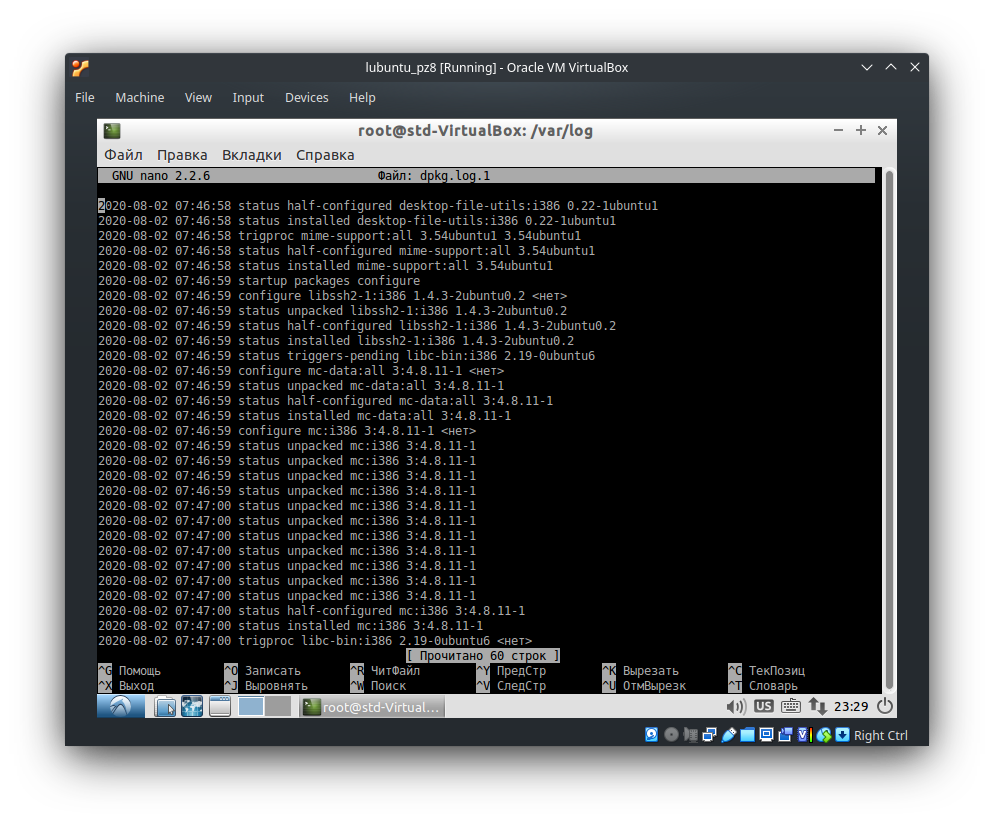
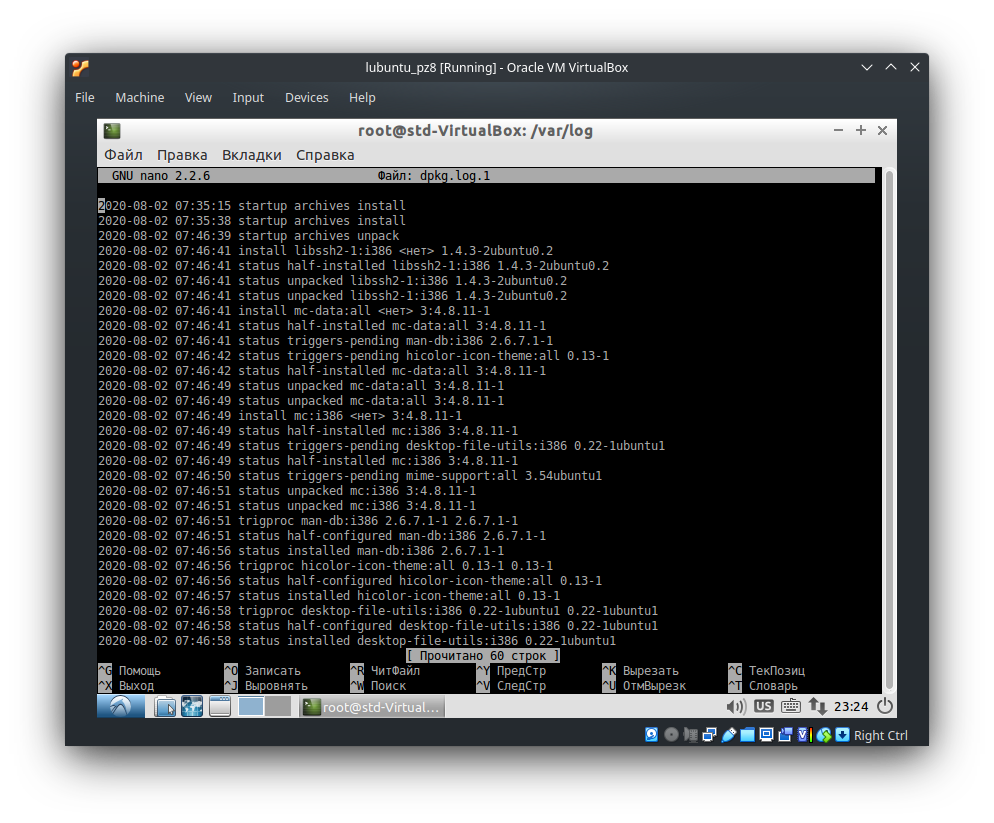
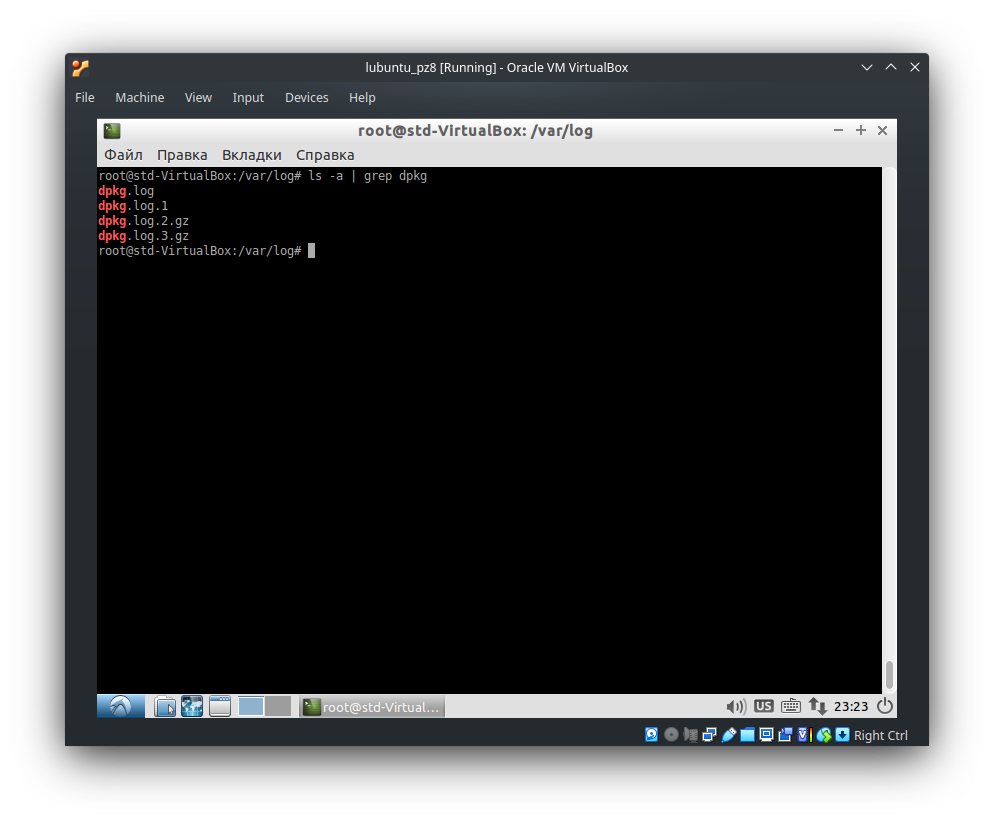
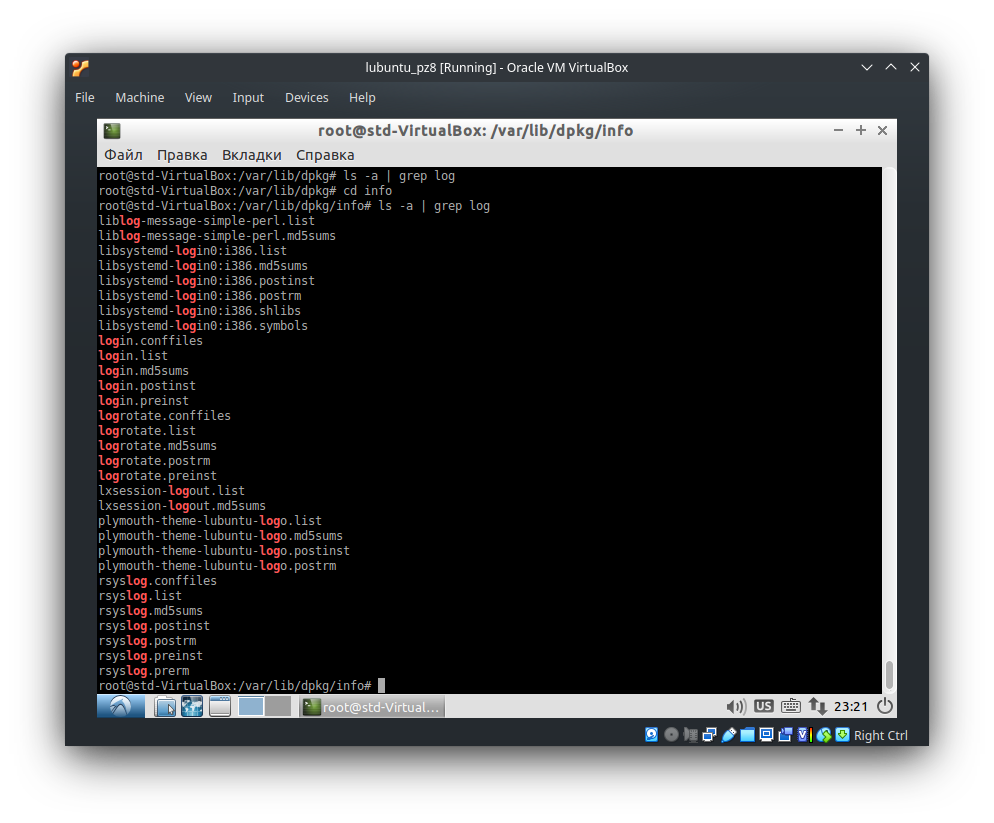
1) Выполнить dpkg –l | more. Используя пробел листайте экраны.



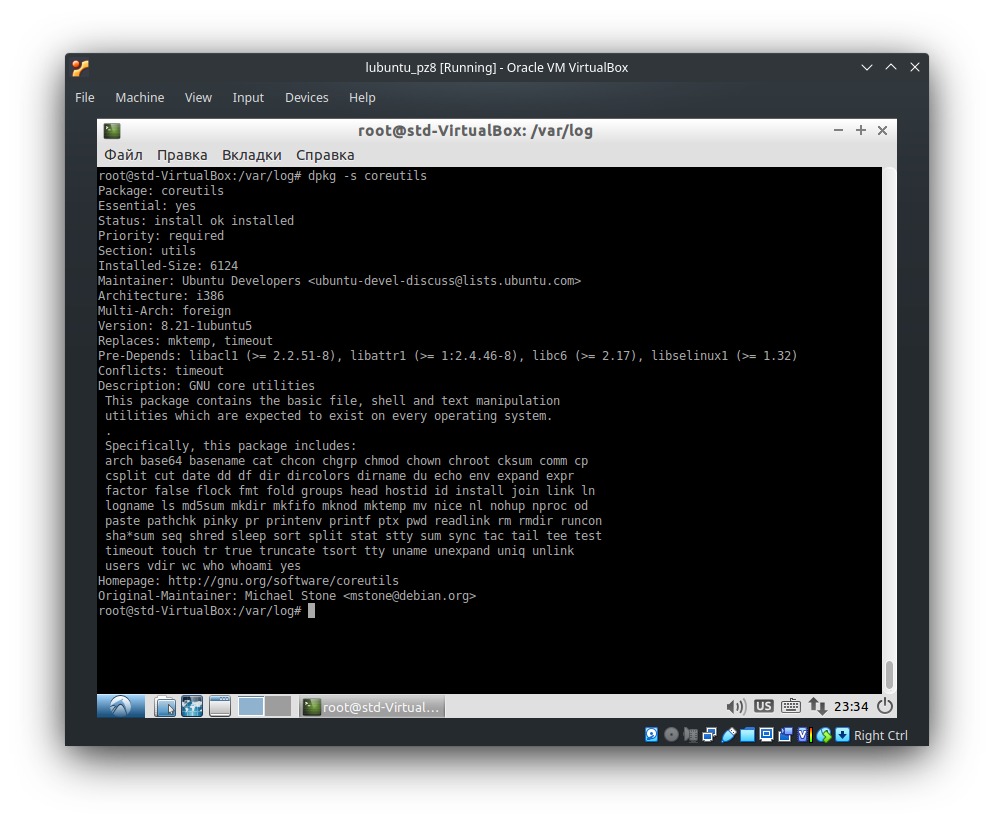
Эта команда выдает сведения о пакетах, их версиях и краткую информацию о назначении каждого пакета. Можно вывести эту информацию в файл, тогда потребуется выполнить команду dpkg –l > имя\_файла.



Используя какое-либо средство навигации файловой системой просмотрите содержимое каталога /var/lib/dpkg/info и файла /var/log/dpkg.log и его архивные копии.



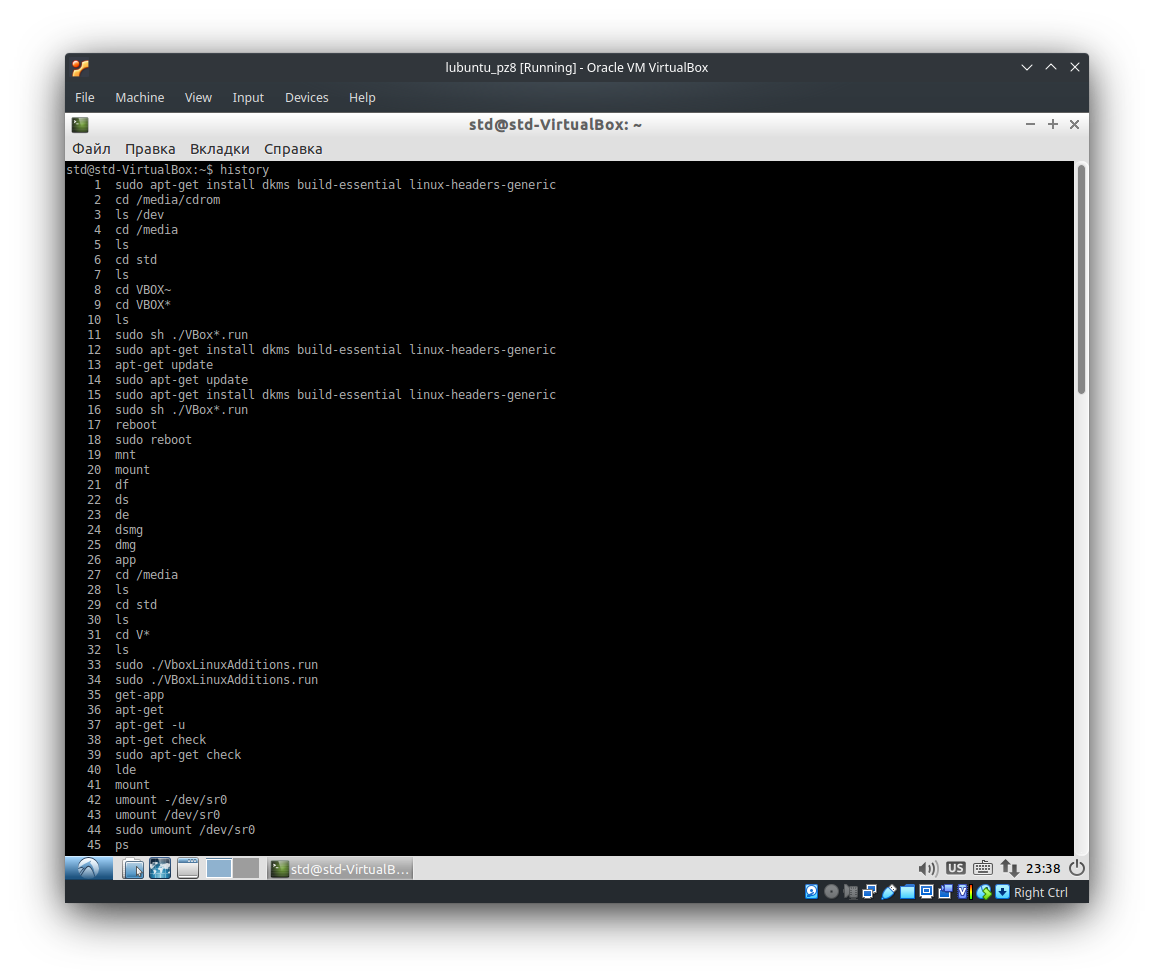
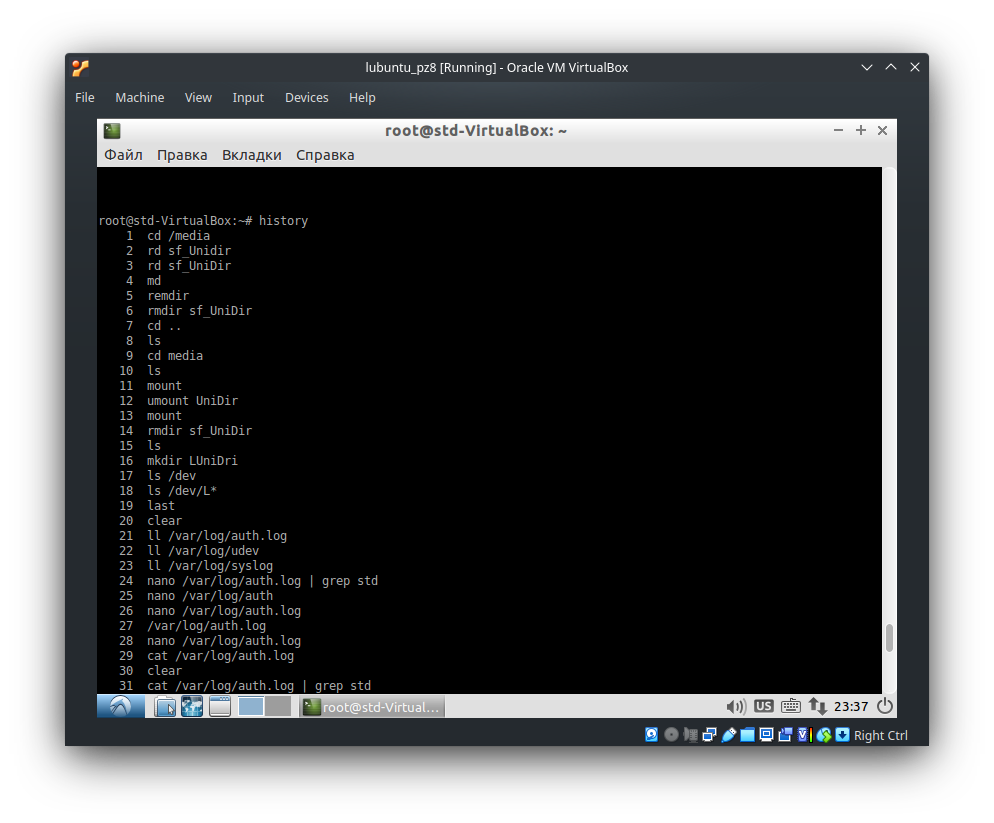
Используя указанные средства найдите информацию об обстоятельствах установки пакета MC.



**Задание 5. Просмотр файла истории команд.**

Интерпретатор команд ведет файл истории. Для того чтобы просмотреть историю команд необходимо выполнить команду history. Файл, содержащий историю команд называется .bash\_history. Он находится в домашней директории пользователя.

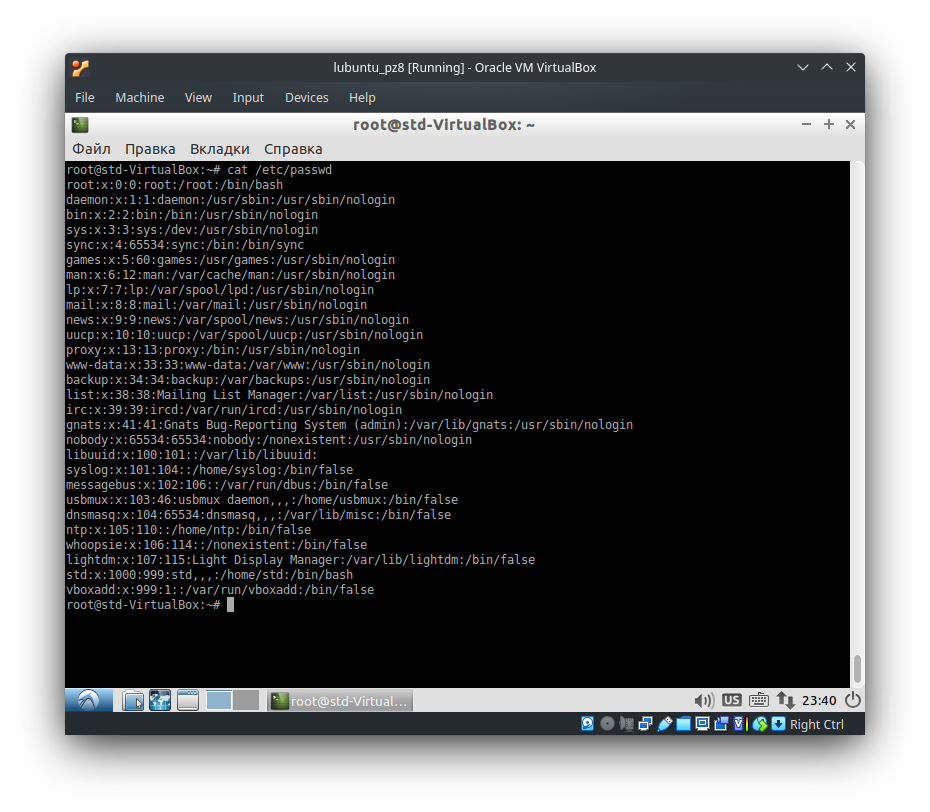
Просмотреть файл истории команд его для пользователей root и std.



**Проверьте себя на полноту фиксации лекционного материала.**

Самостоятельно найдите:

1. Список пользователей системы



1. Список автоматически монтируемых файловых систем

