

## Born2beroot - ecole42

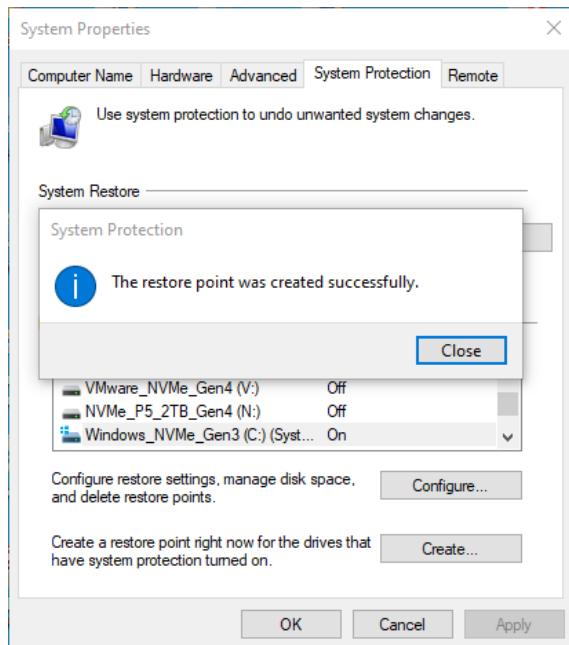
Notebook: Linux  
Created: 2023-11-26 16:23 Updated: 2023-12-05 19:23  
Author: Pete Meechan  
URL: [https://www.server-world.info/en/note?os=Debian\\_12&p=pam&f=1](https://www.server-world.info/en/note?os=Debian_12&p=pam&f=1)

---

### Create System Restore Point

Create a system restore point to allow recovery in case things go seriously wrong. A full disk backup is a better option, but takes considerably longer!

Windows Key+i -> System-> About then choose Advanced System Settings. From the System Protection tab, click Create.



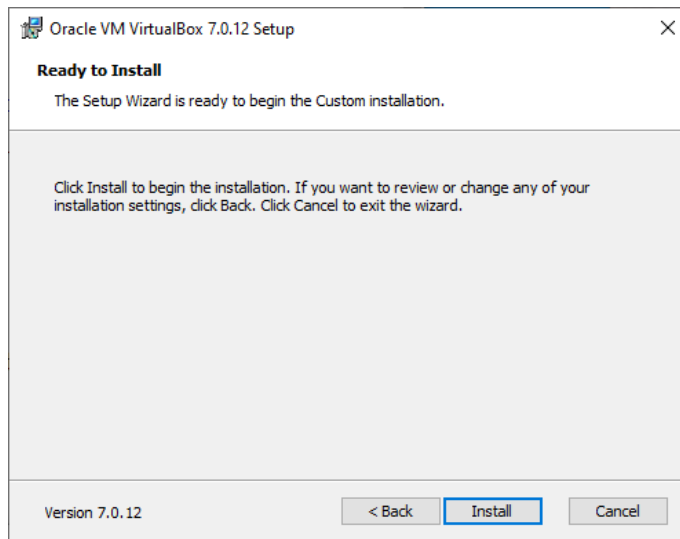
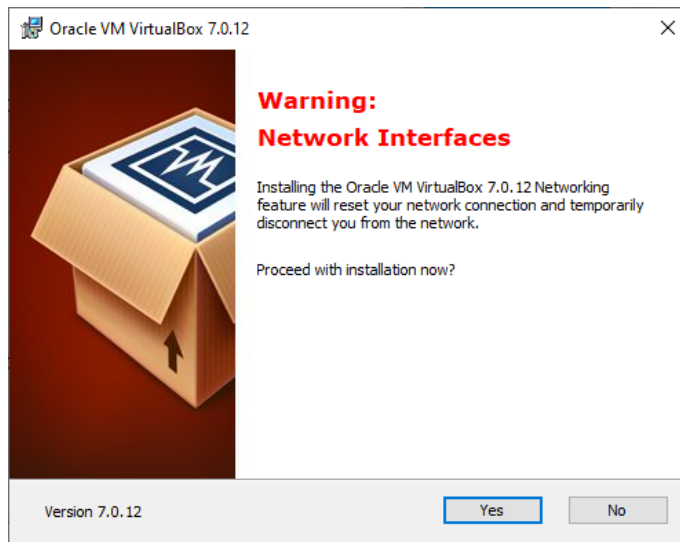
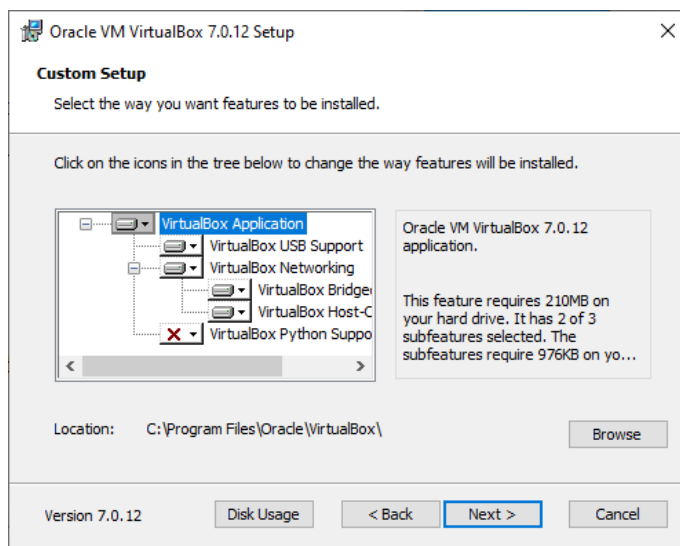
### Download Virtual Box and install

Download from <https://www.virtualbox.org> - choose the Windows hosts download e.g. VirtualBox-7.0.12-159484-Win.exe

Execute installer (As Administrator or user with Administrator authority)



Optional - disable the Python support if not required (I don't have Python installed on my desktop so I disabled it)





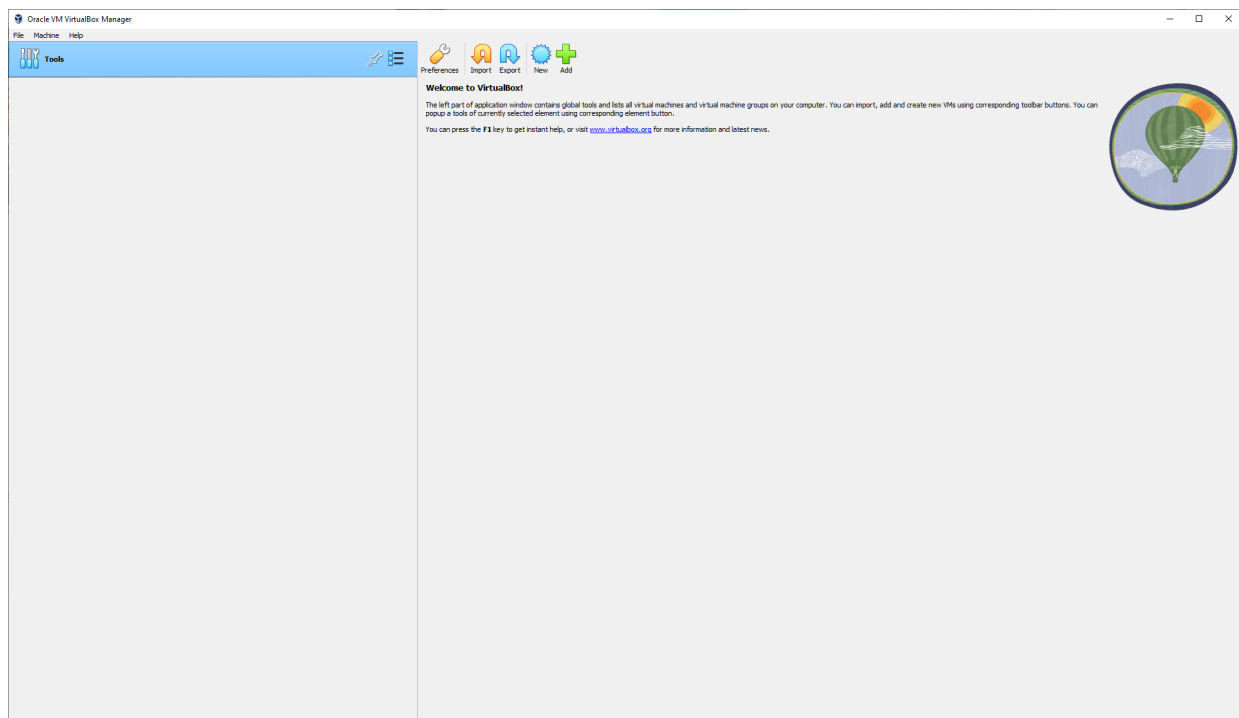
Create a folder for the VirtualBox virtual machines (VMs) e.g. c:\VirtualBox (my examples use V:\VirtualBox)

## Download debian linux

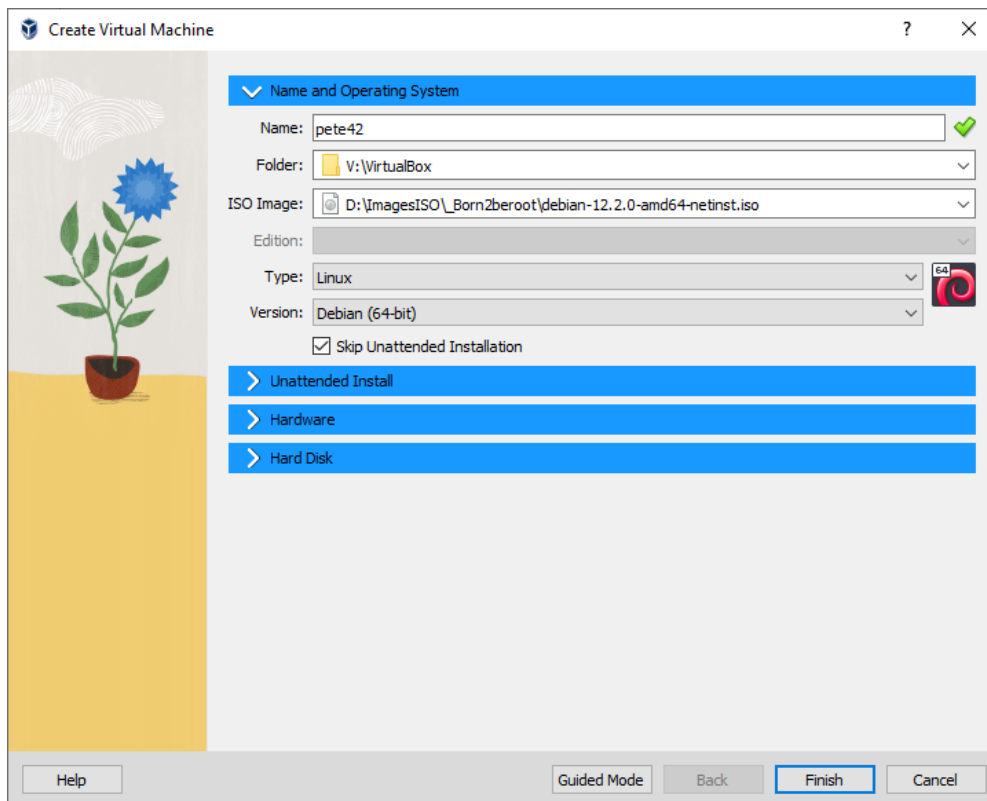
Download debian linux from <https://www.debian.org> and click Download to download debian linux as an ISO (disk) image

## Install and configure debian linux

Start VirtualBox and install debian linux as shown below



Click New icon on menu bar and then click "Expert Mode" in the pop-up window to show the following screen - make sure you check the Skip Unattended Install box



**Create Virtual Machine**

**Name and Operating System**

Name:

Folder:

ISO Image:

Edition:

Type:

Version:

☒ Skip Unattended Installation

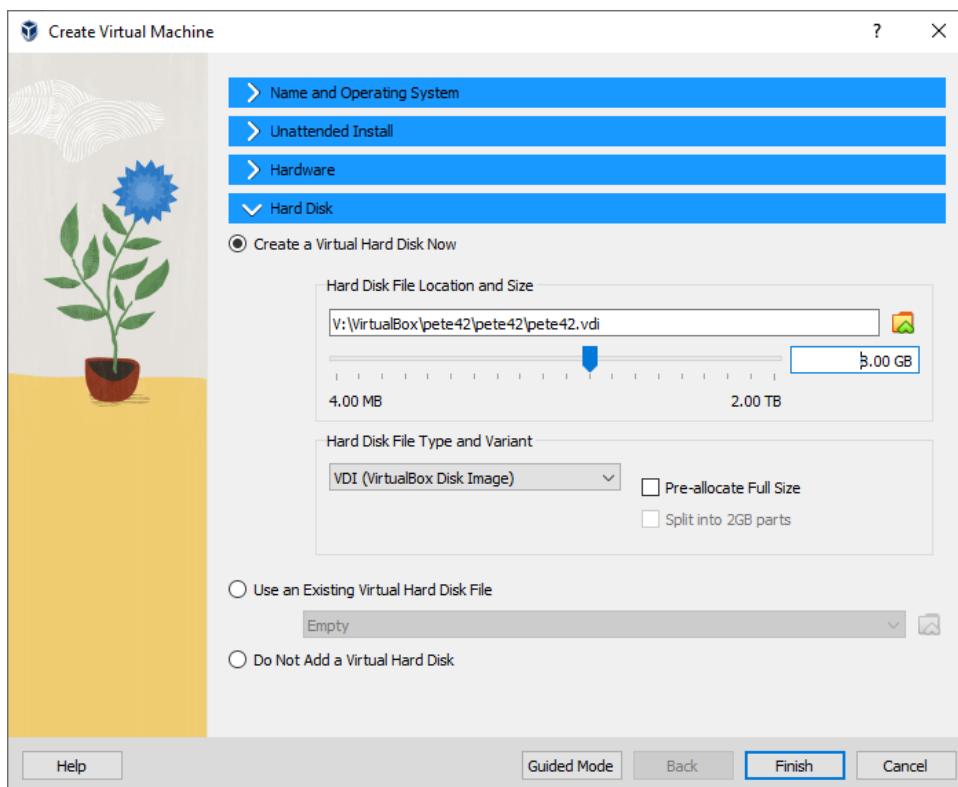
> Unattended Install

> Hardware

> Hard Disk

Help Guided Mode Back Finish Cancel

Then click the hard disk tab and set disk space size to 8.0GB and then click Finish



**Create Virtual Machine**

> Name and Operating System

> Unattended Install

> Hardware

**> Hard Disk**

☒ Create a Virtual Hard Disk Now

Hard Disk File Location and Size

4.00 MB 8.00 GB 2.00 TB

Hard Disk File Type and Variant

☐ Pre-allocate Full Size

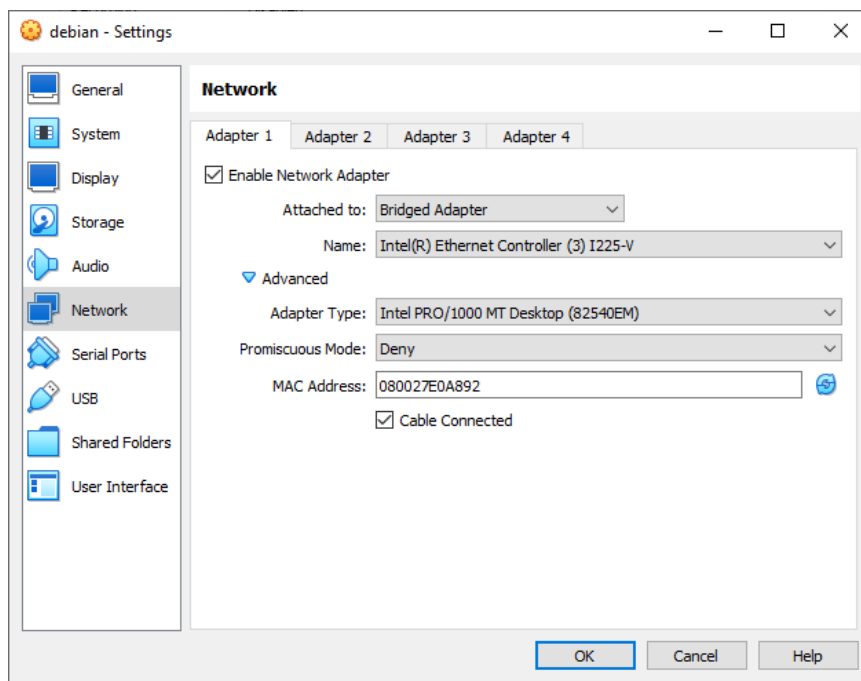
☐ Split into 2GB parts

☐ Use an Existing Virtual Hard Disk File

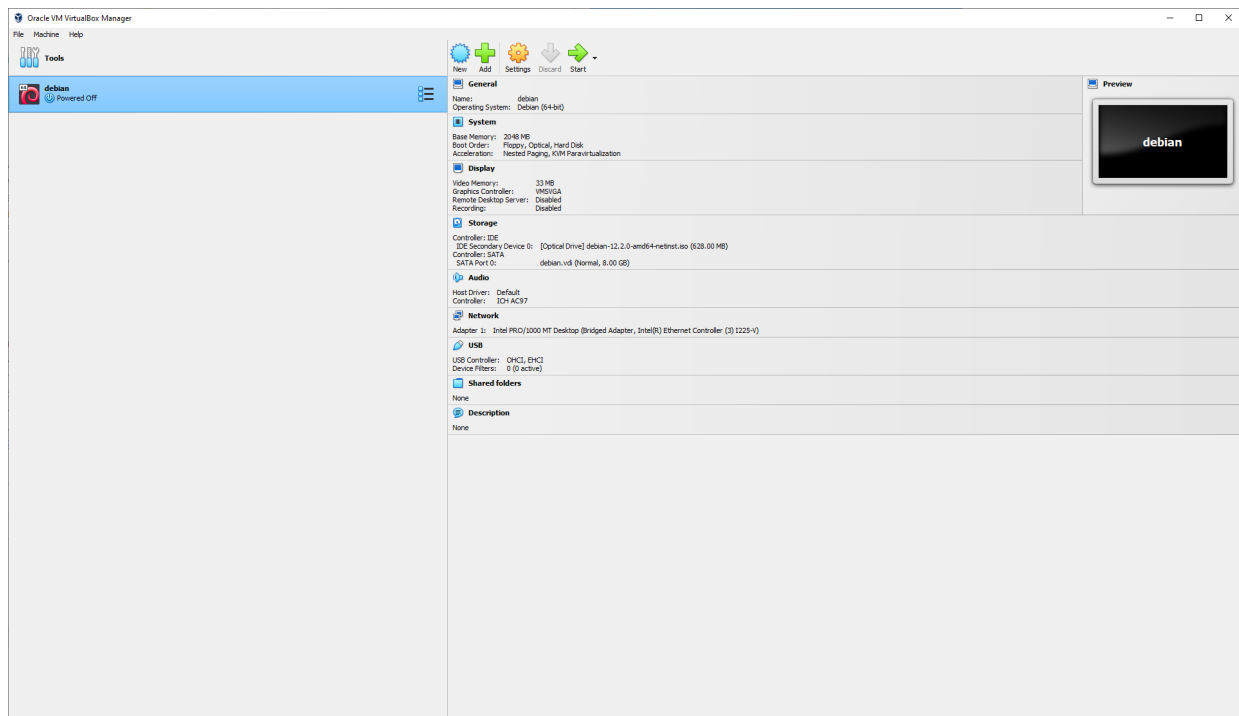
☐ Do Not Add a Virtual Hard Disk

Help Guided Mode Back Finish Cancel

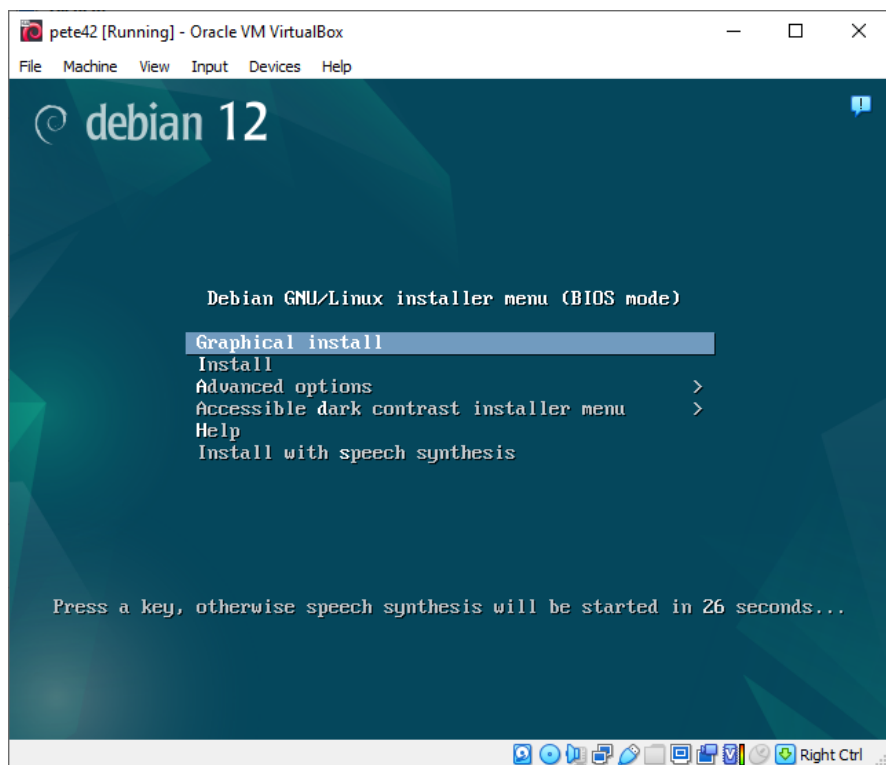
Click Settings and then Network. Enable the network adapter as a Bridged Adapter as this allows the VM access to the internet using the host machine (desktop/laptop) network adapter and also allows the host machine access to the VM. There are many different network options available - more details can be found here <https://www.nakivo.com/blog/virtualbox-network-setting-guide/>



Click Start on the next screen

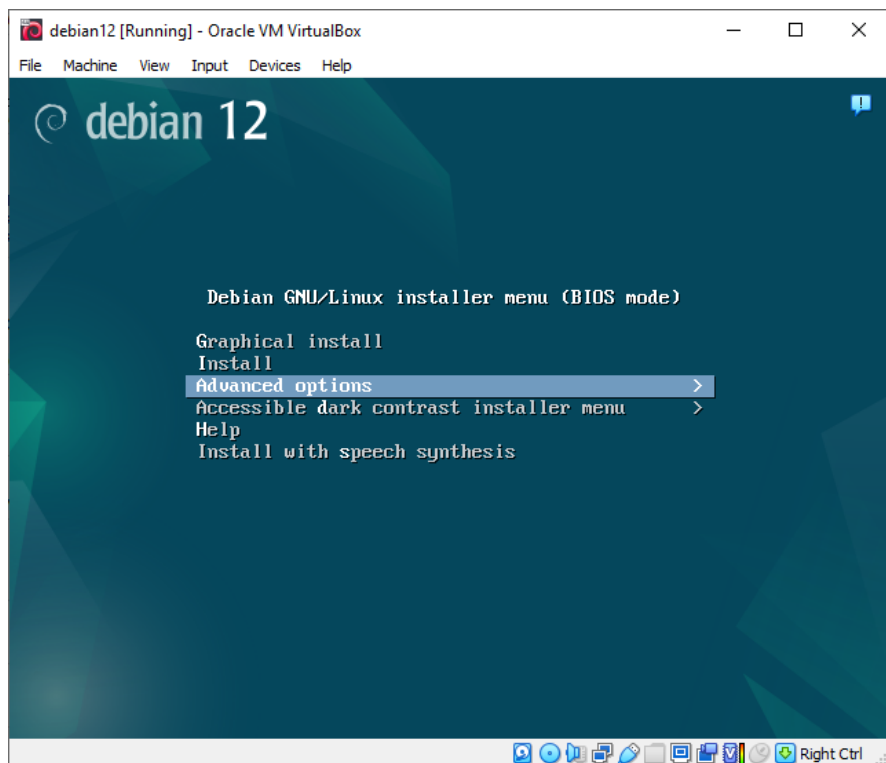


On the screen below press any key on the keyboard to prevent the system automatically installing

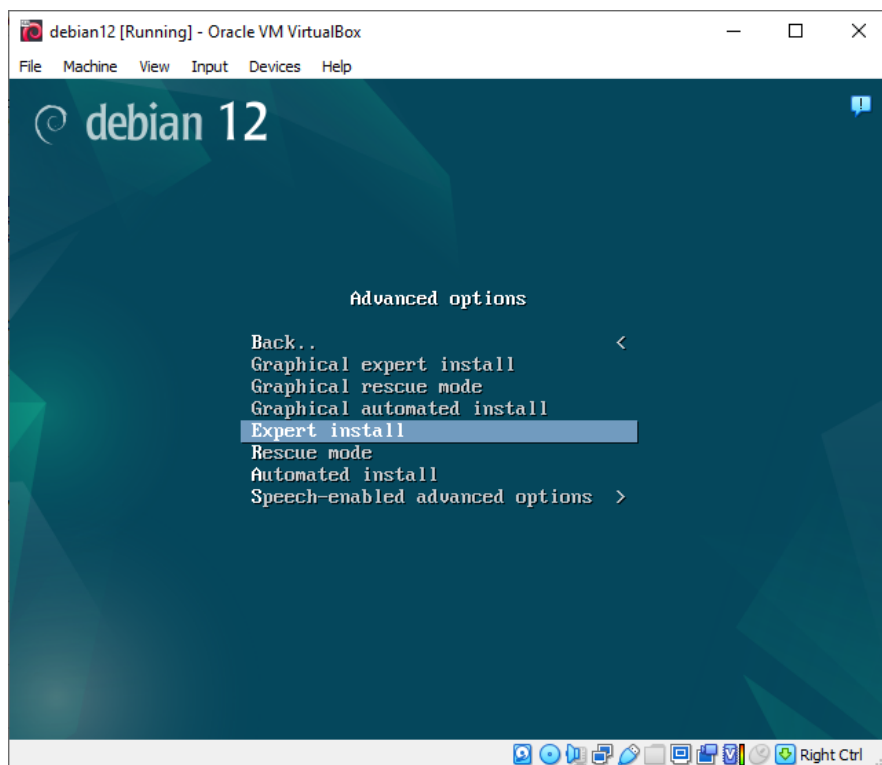


Use the up/down arrows to select the Graphical install option and press enter then follow the screenshots below

To set up the file systems as required it is best to use the Advanced options

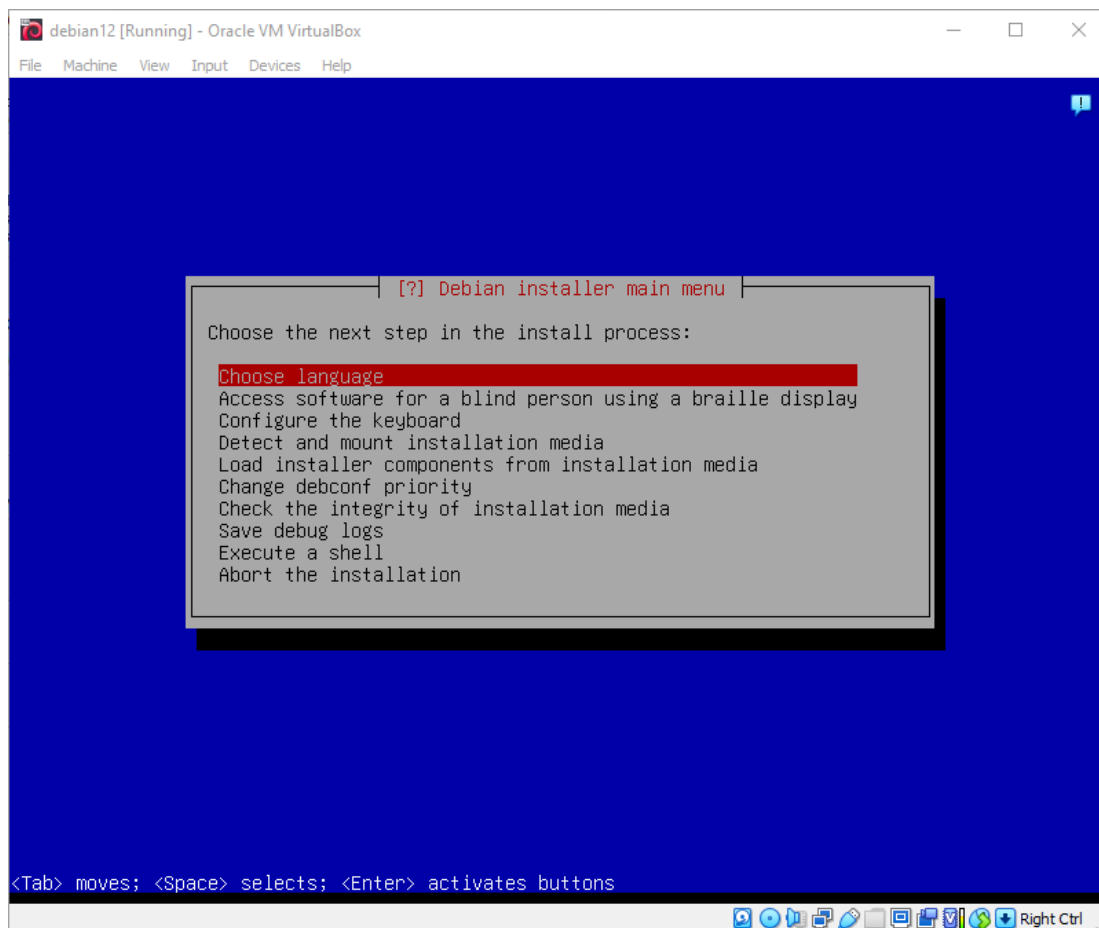


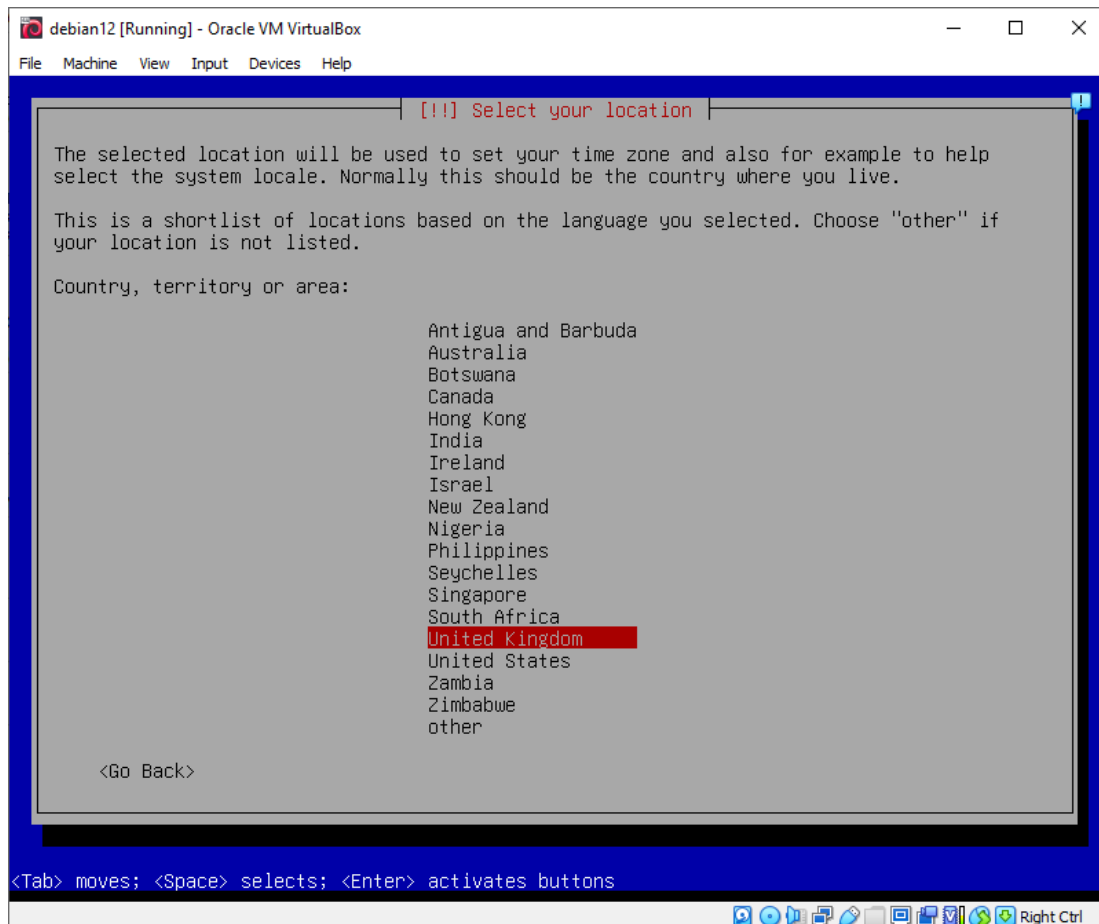
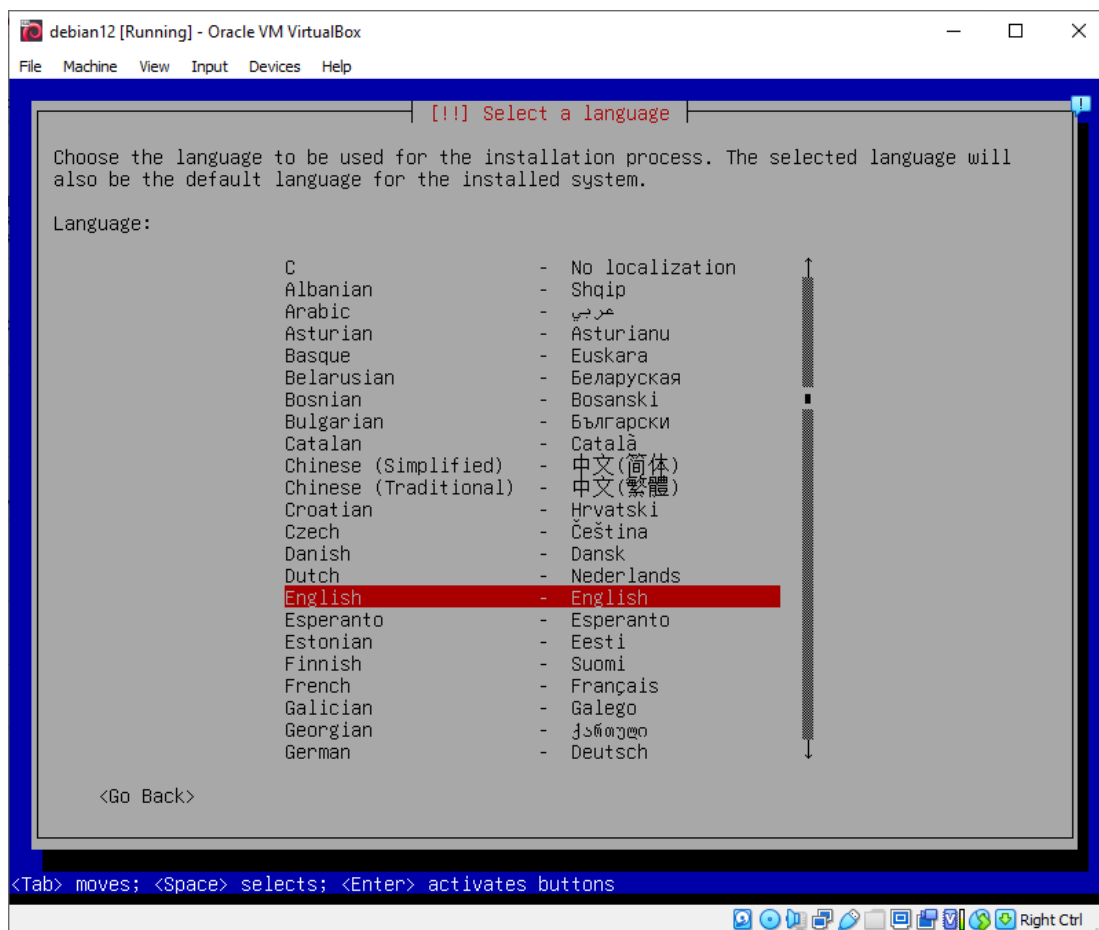
and then choose Expert Install



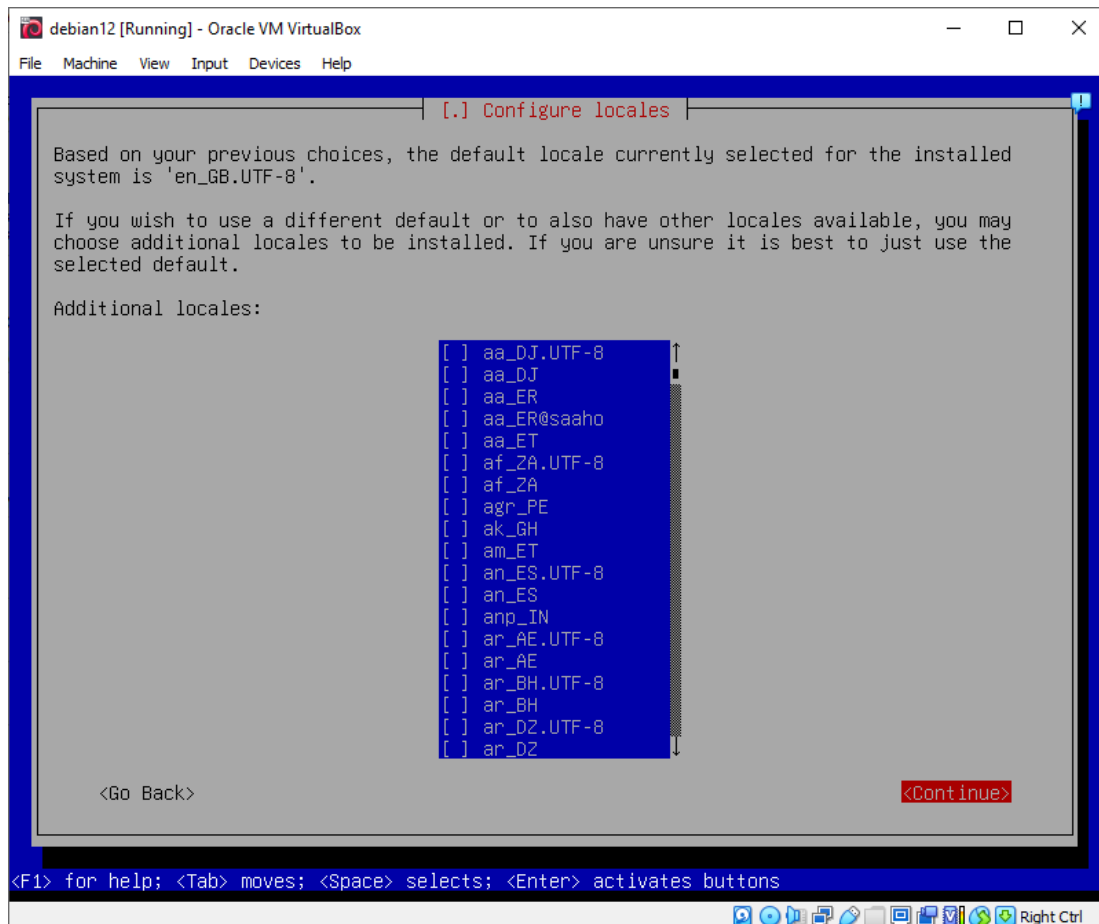
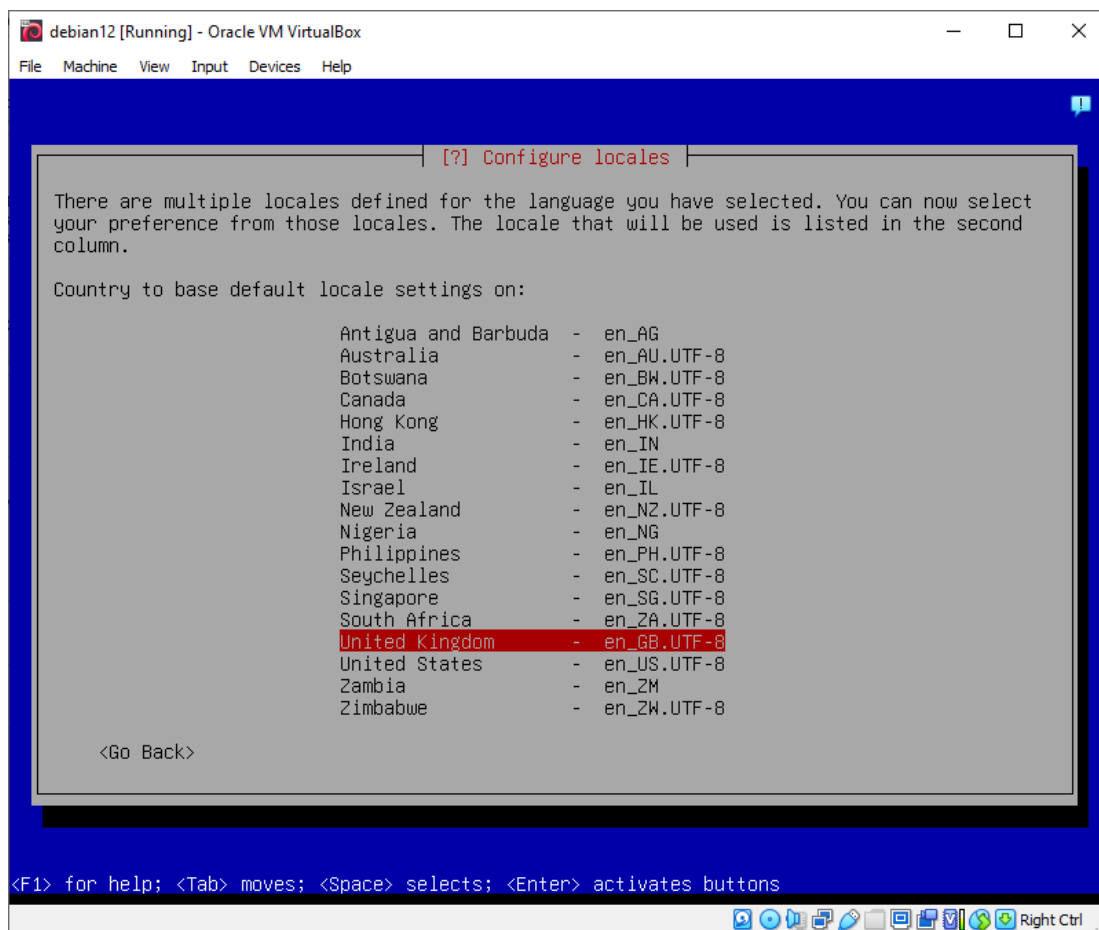
Follow the screenshots below - choosing the language/keyboard etc. suitable for your setup

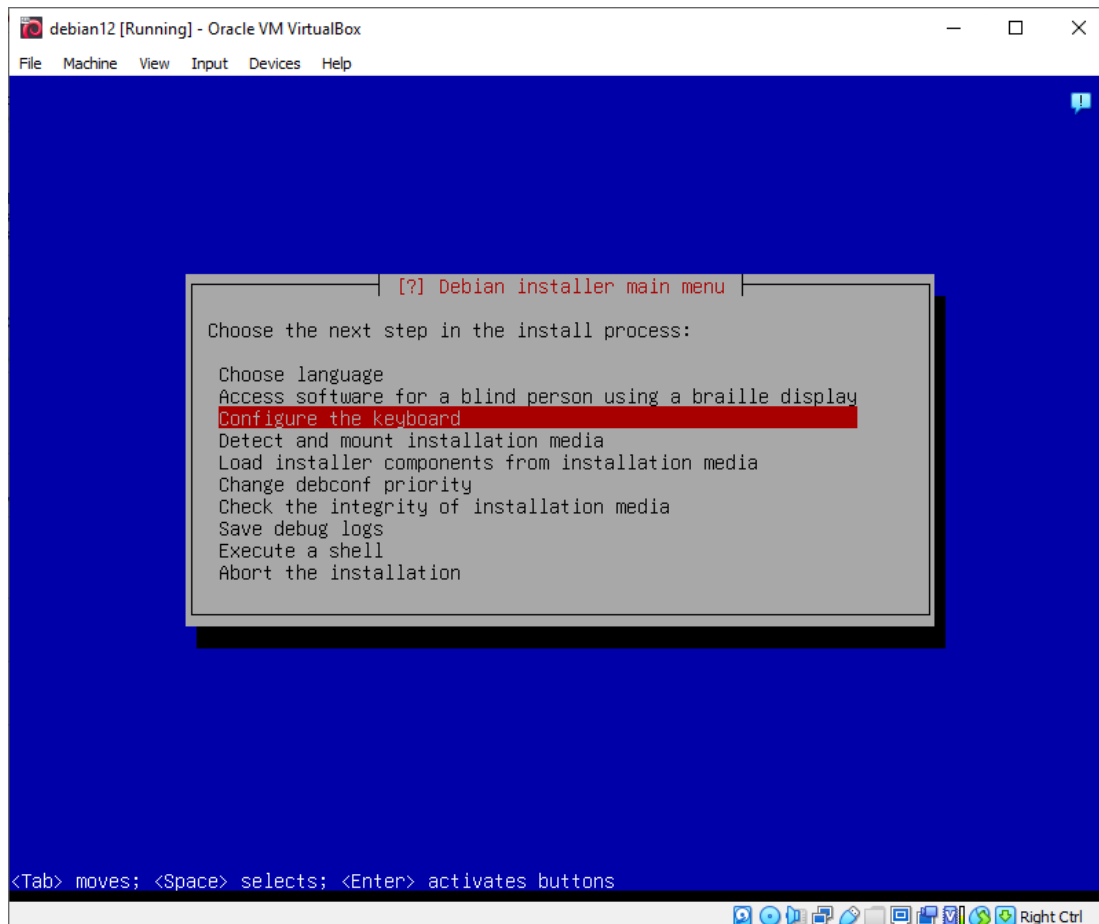
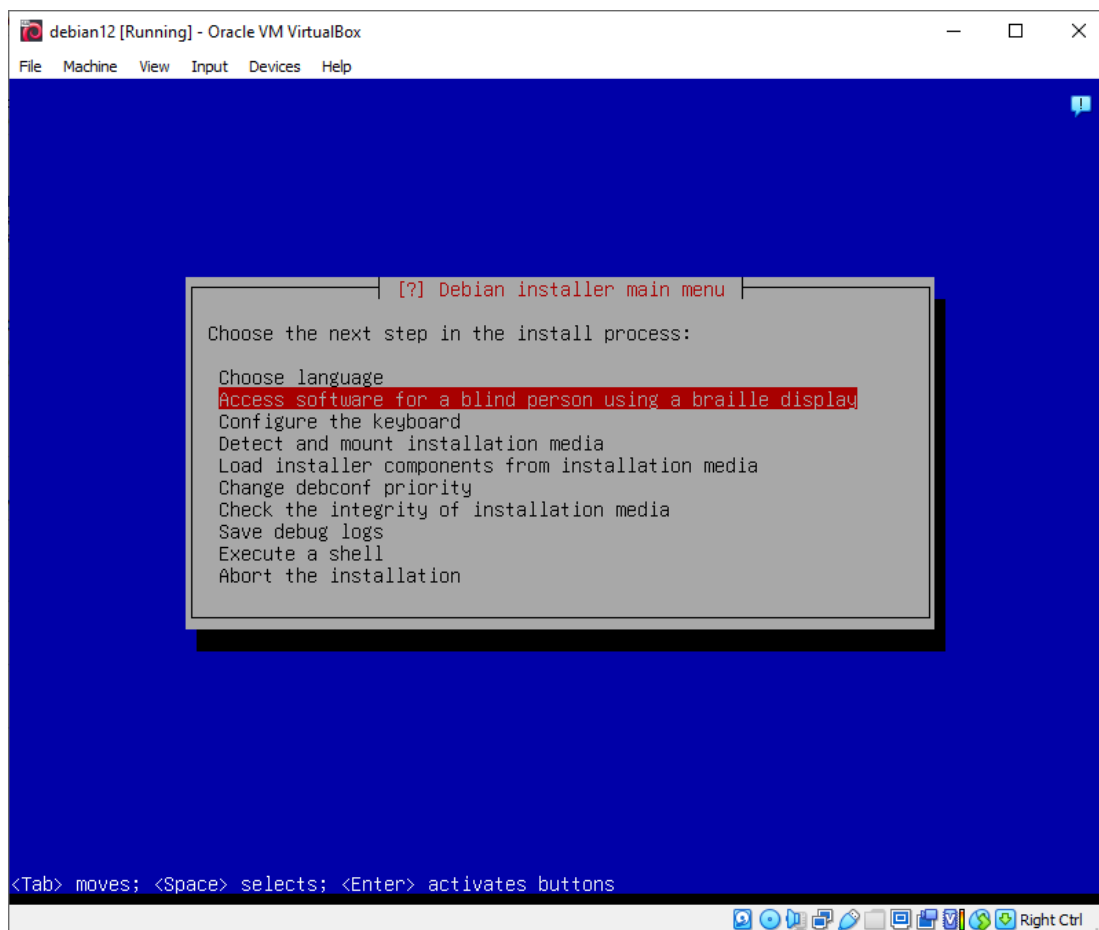
Use the tab key to move between options and the up/down arrow keys to choose the selection and then press space to enable/disable an option or press ENTER to select the option.

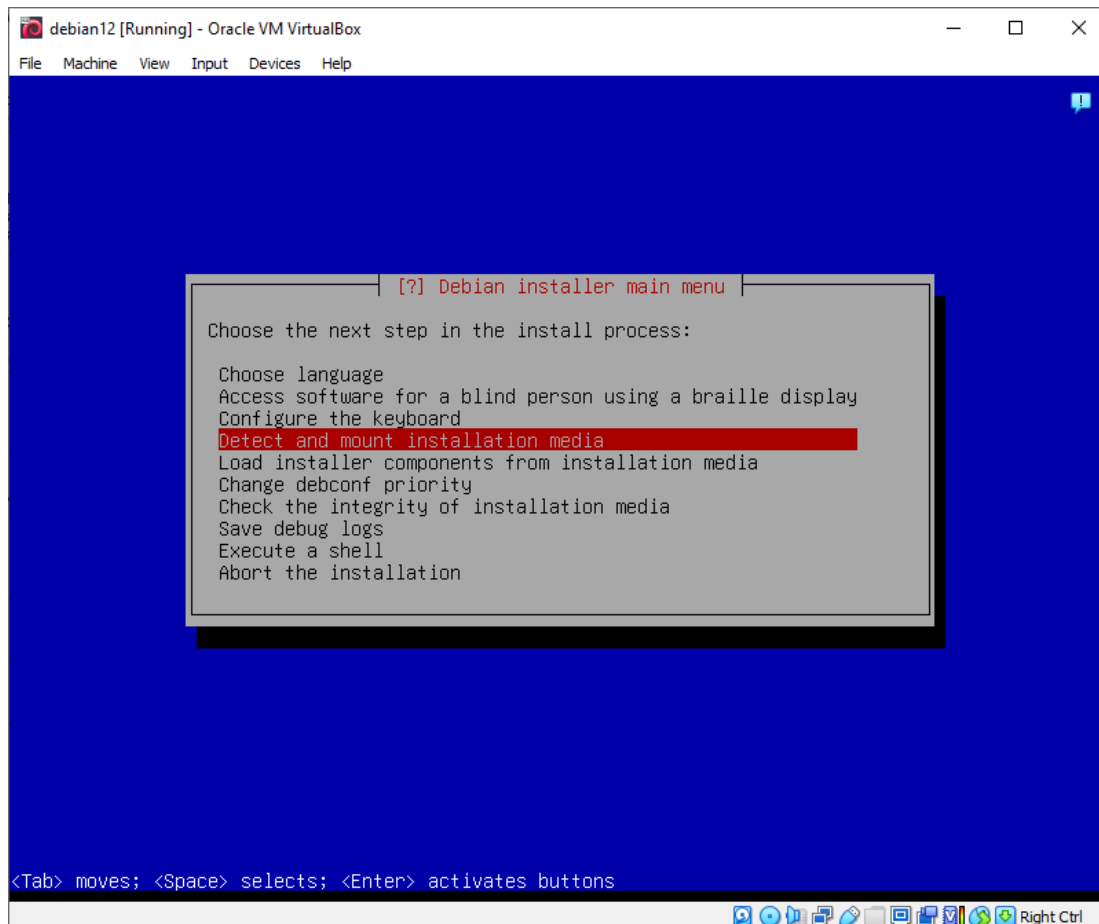
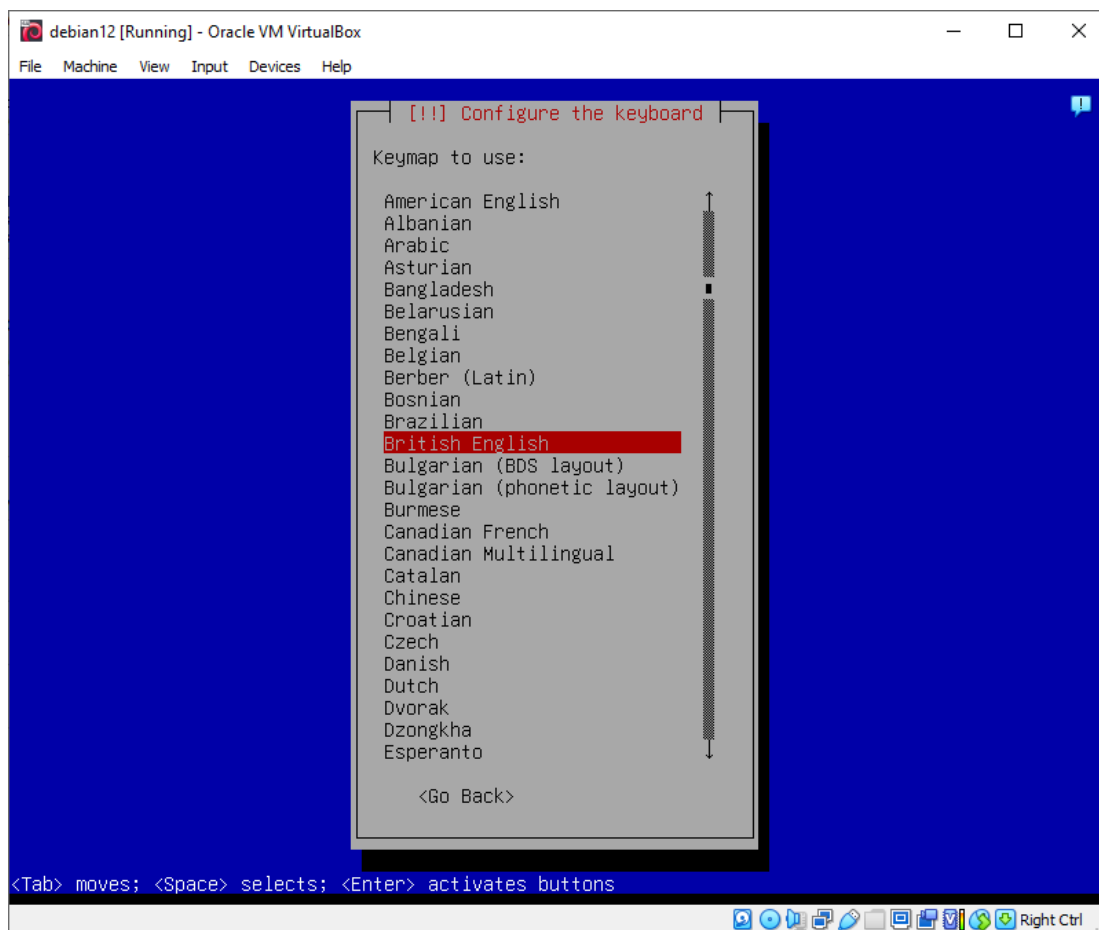


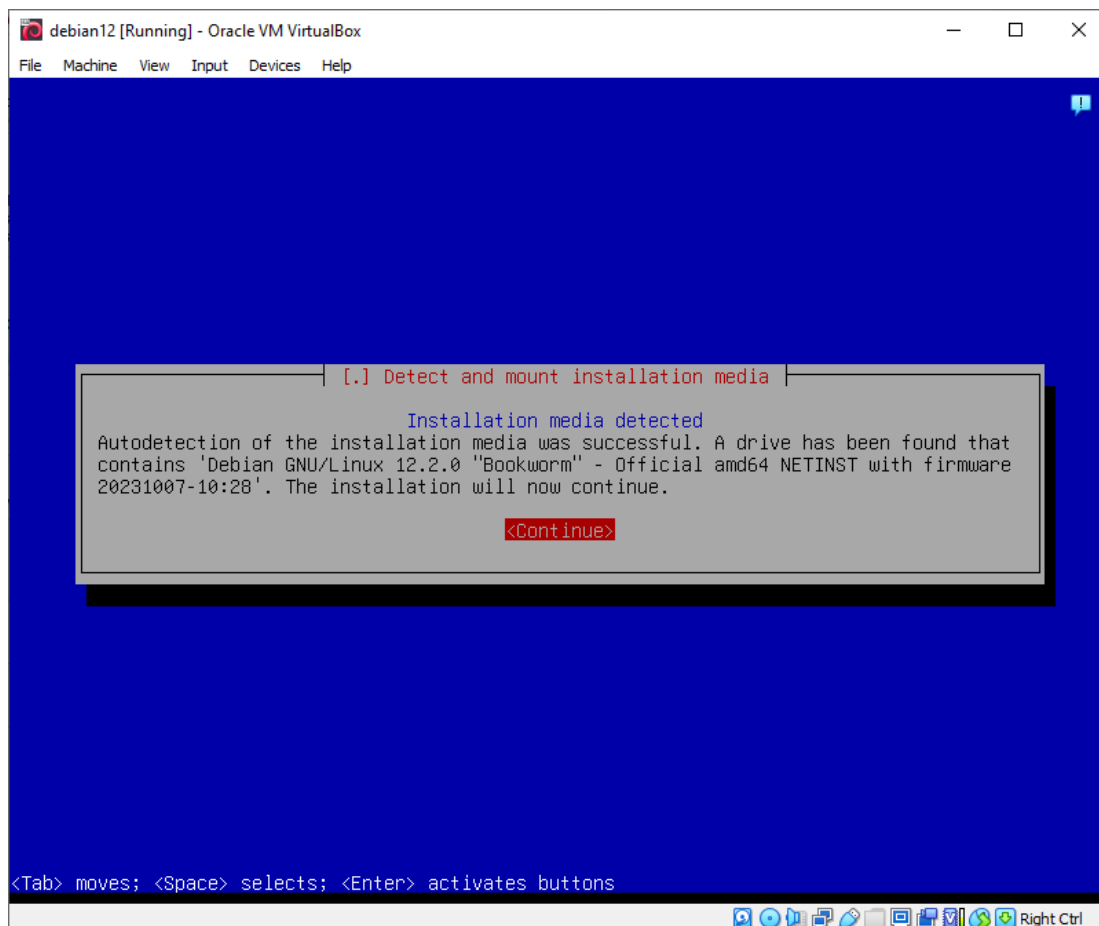
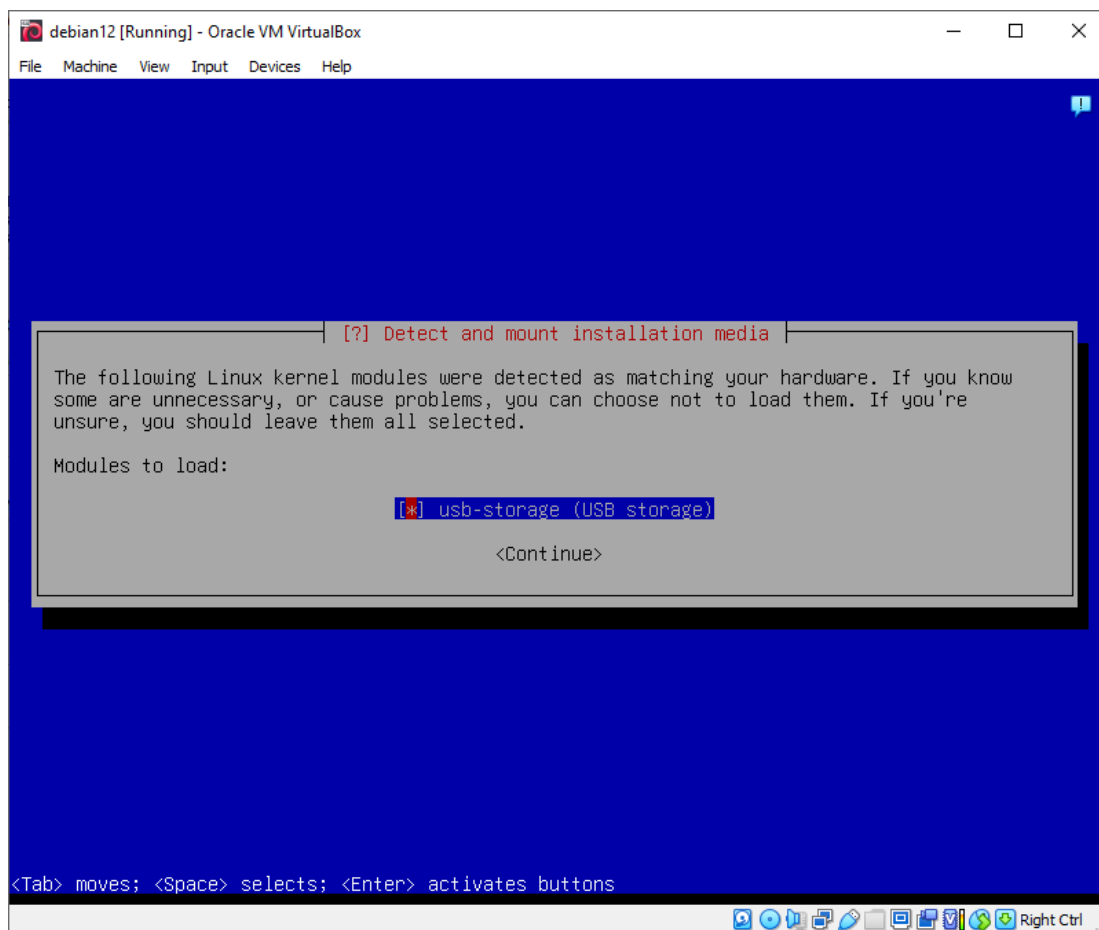


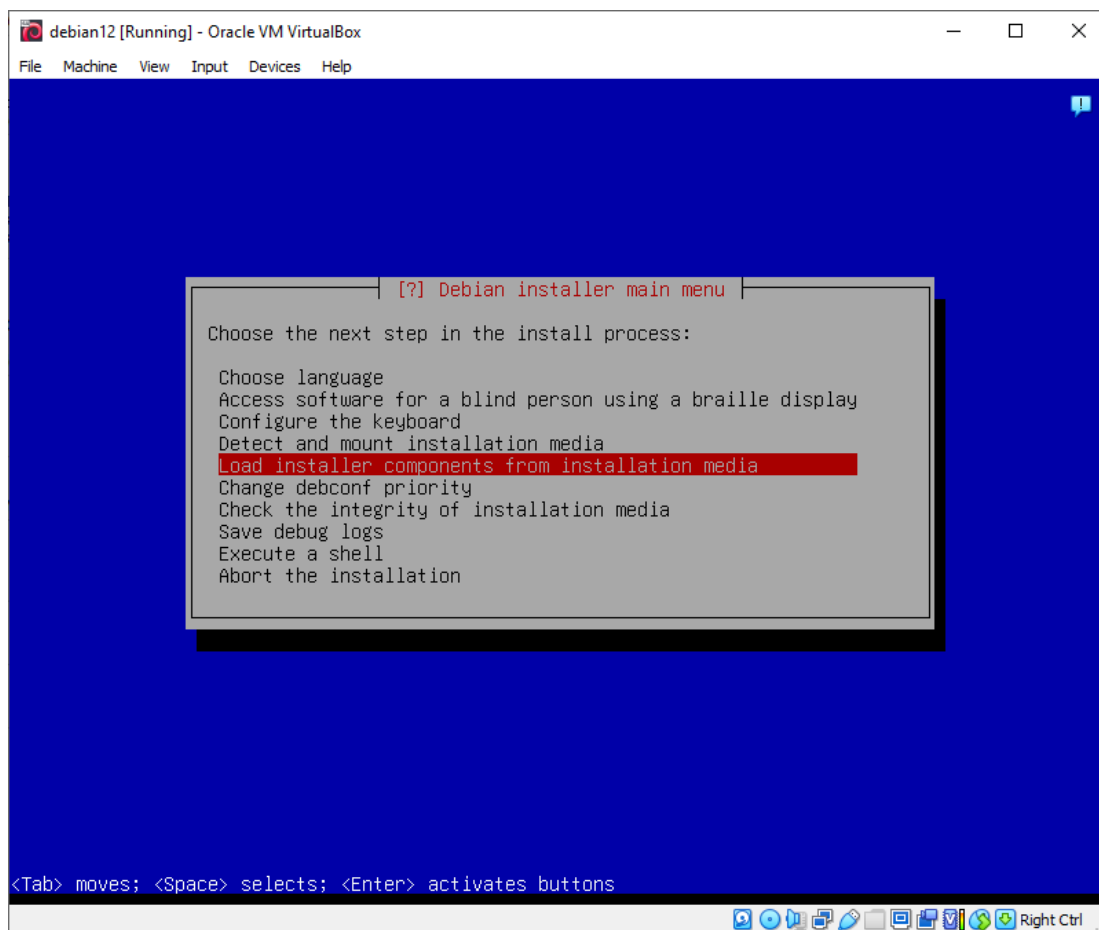




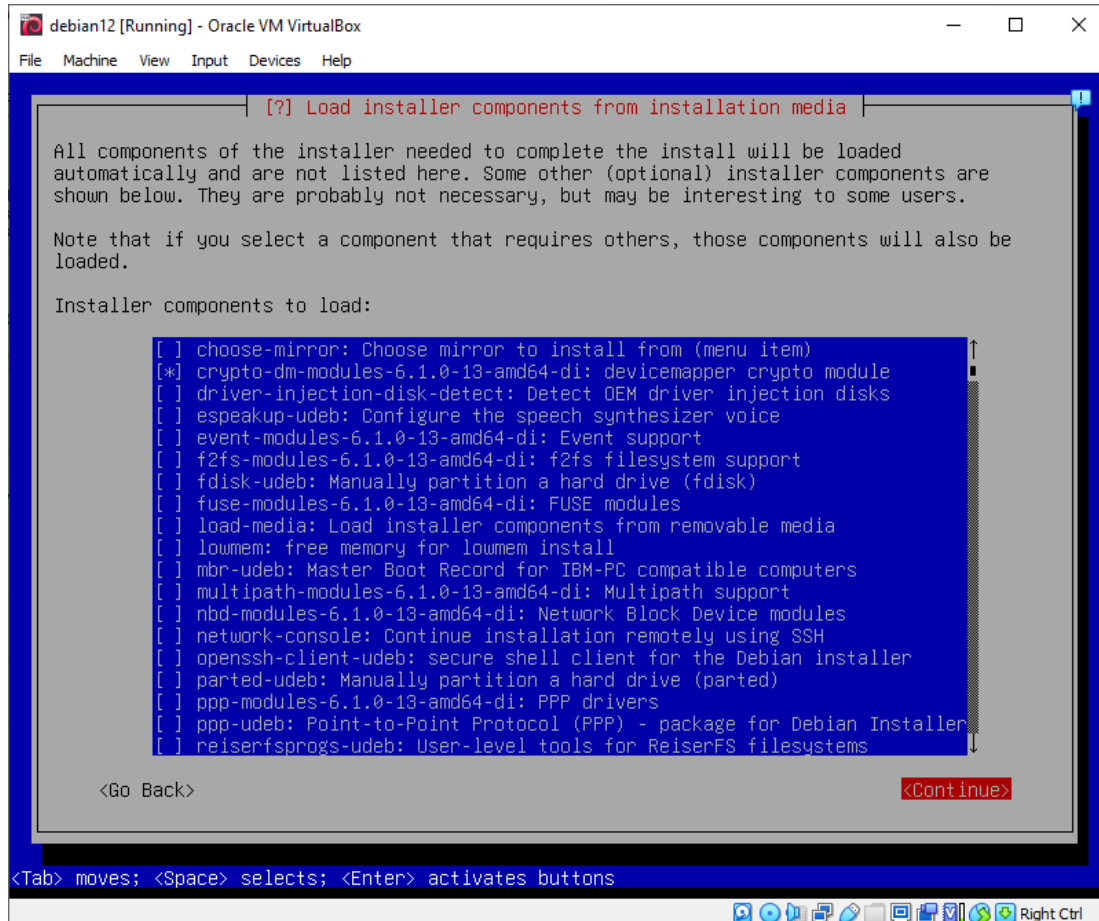


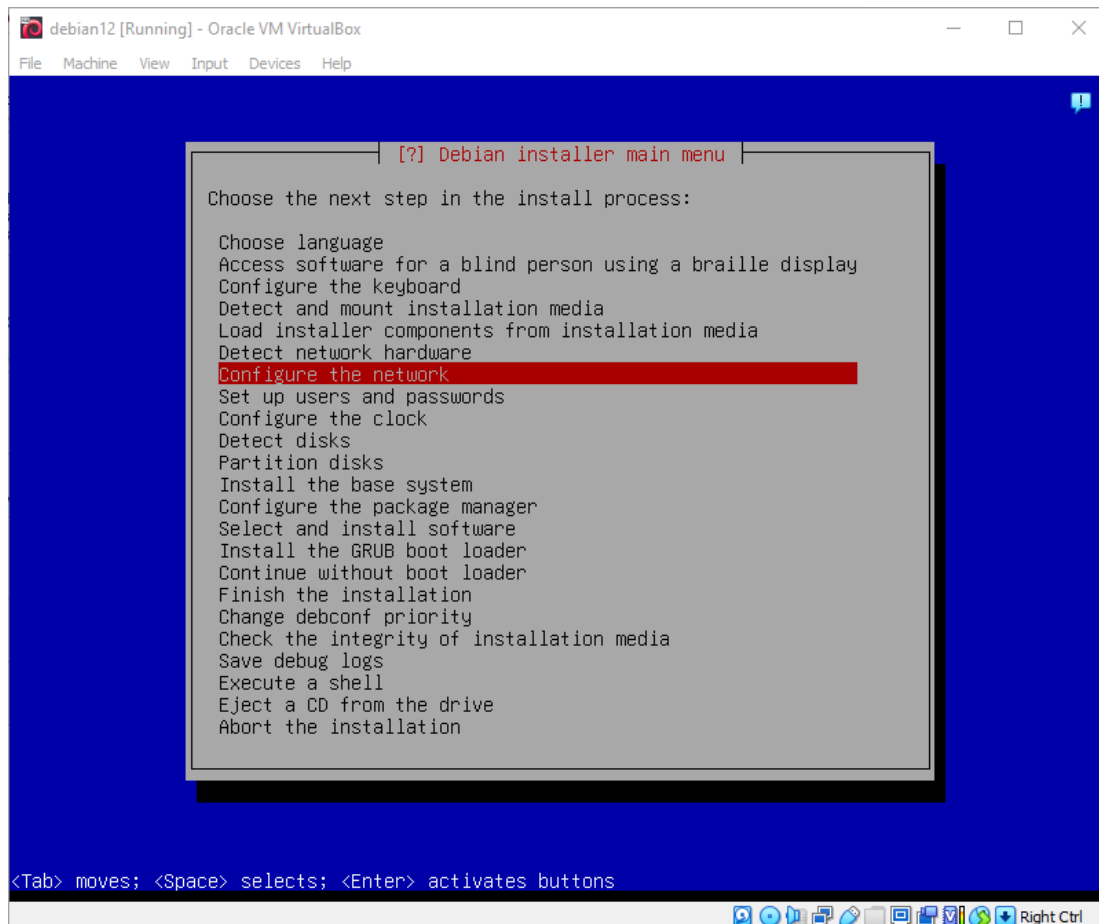
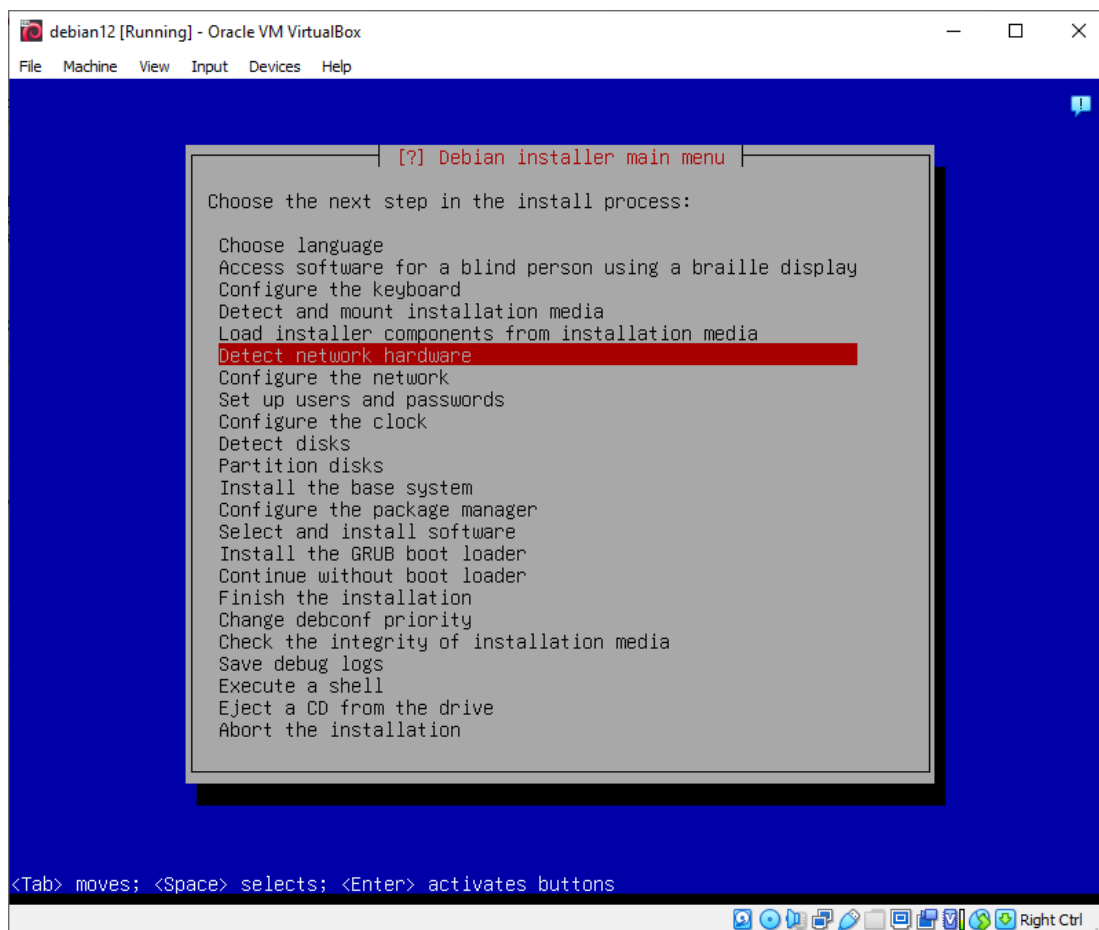


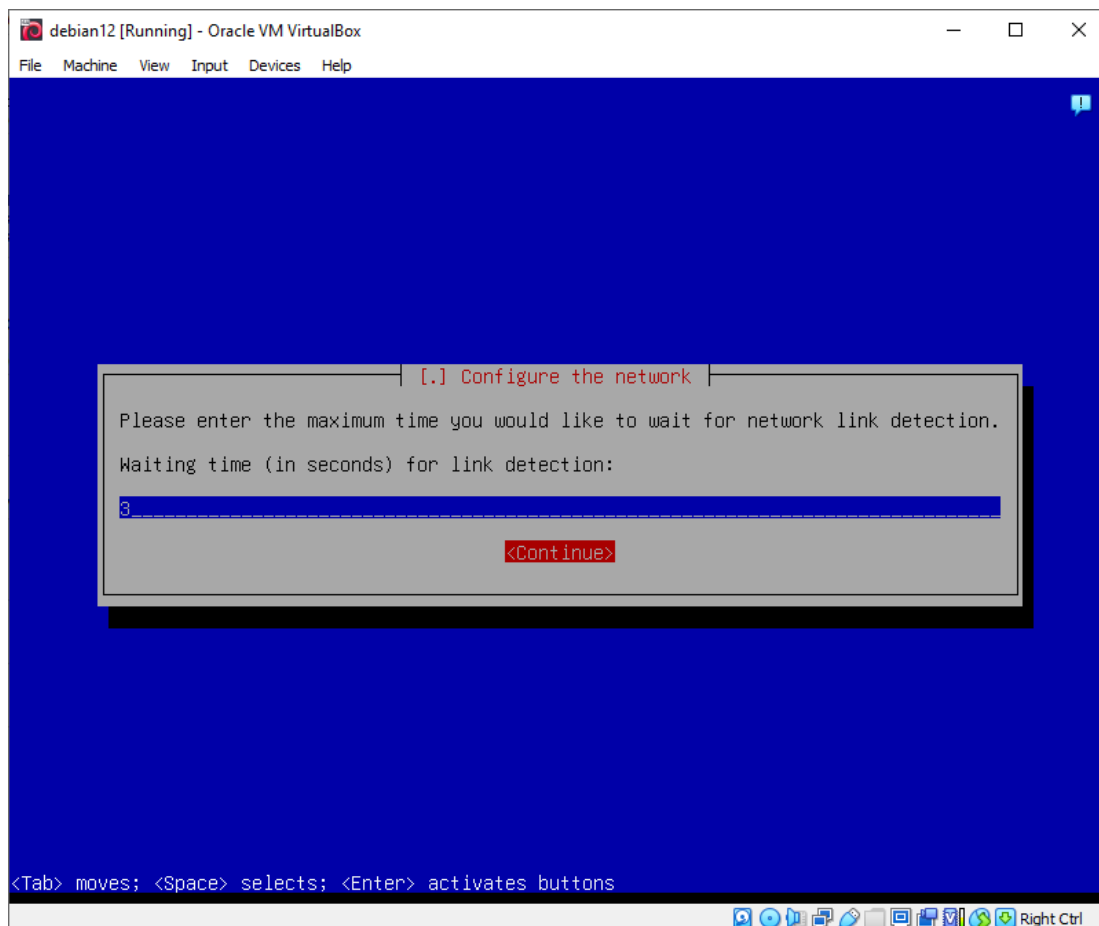
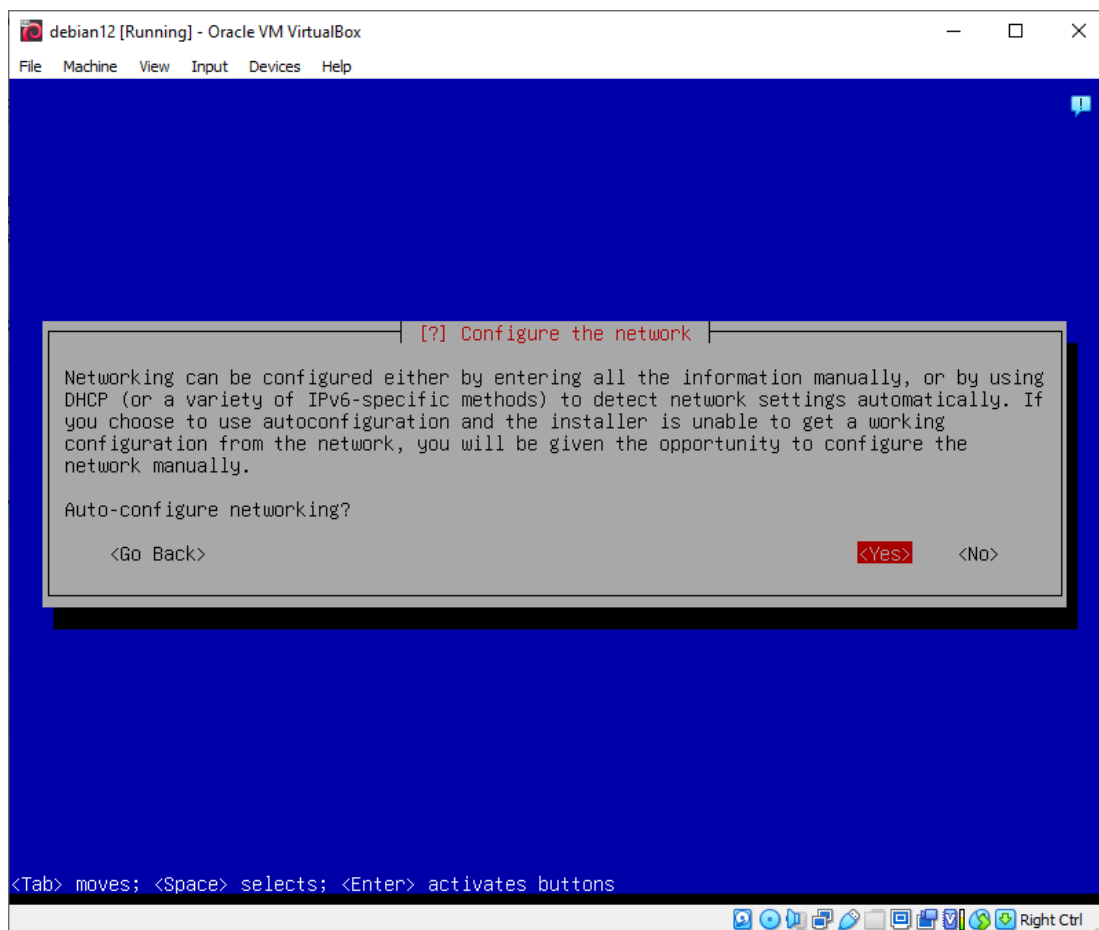




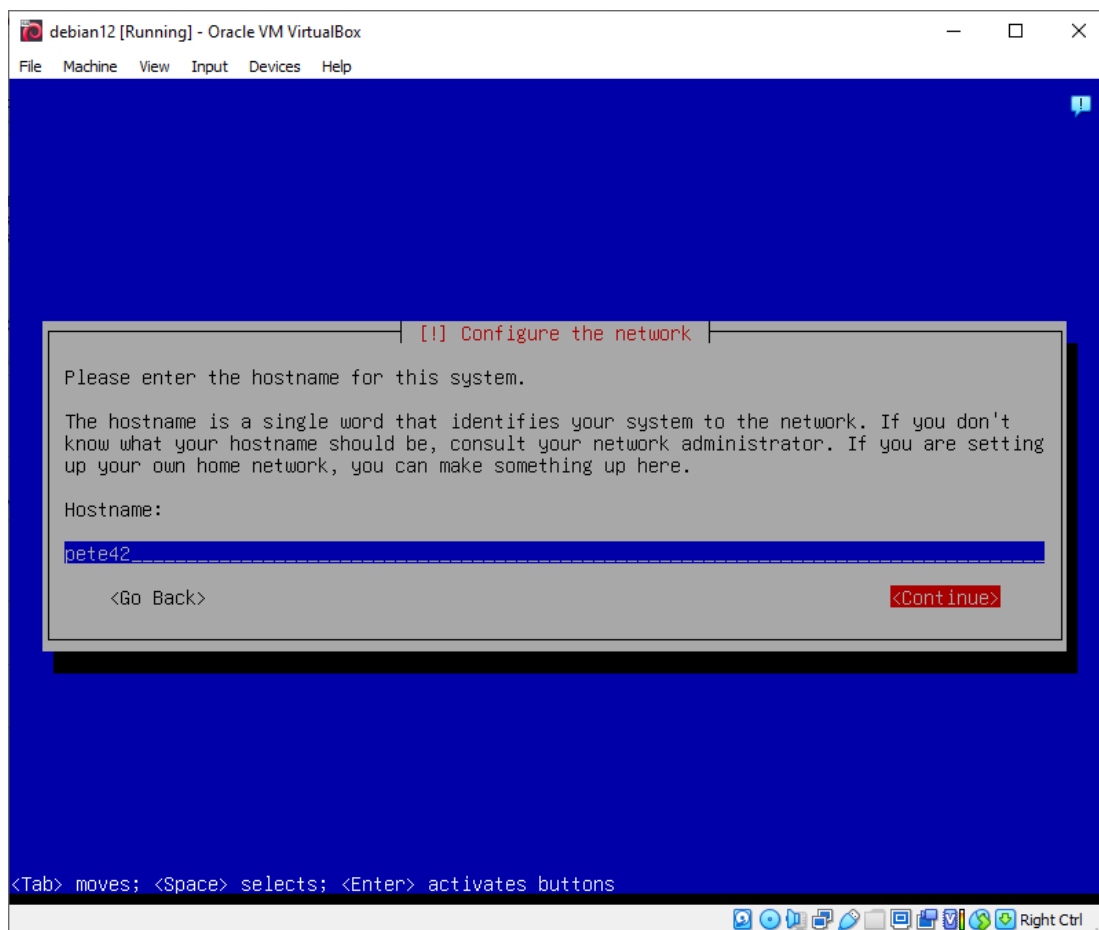
Select the crypto-dm-modules as shown below (use the up/down keys and space to select/unselect)



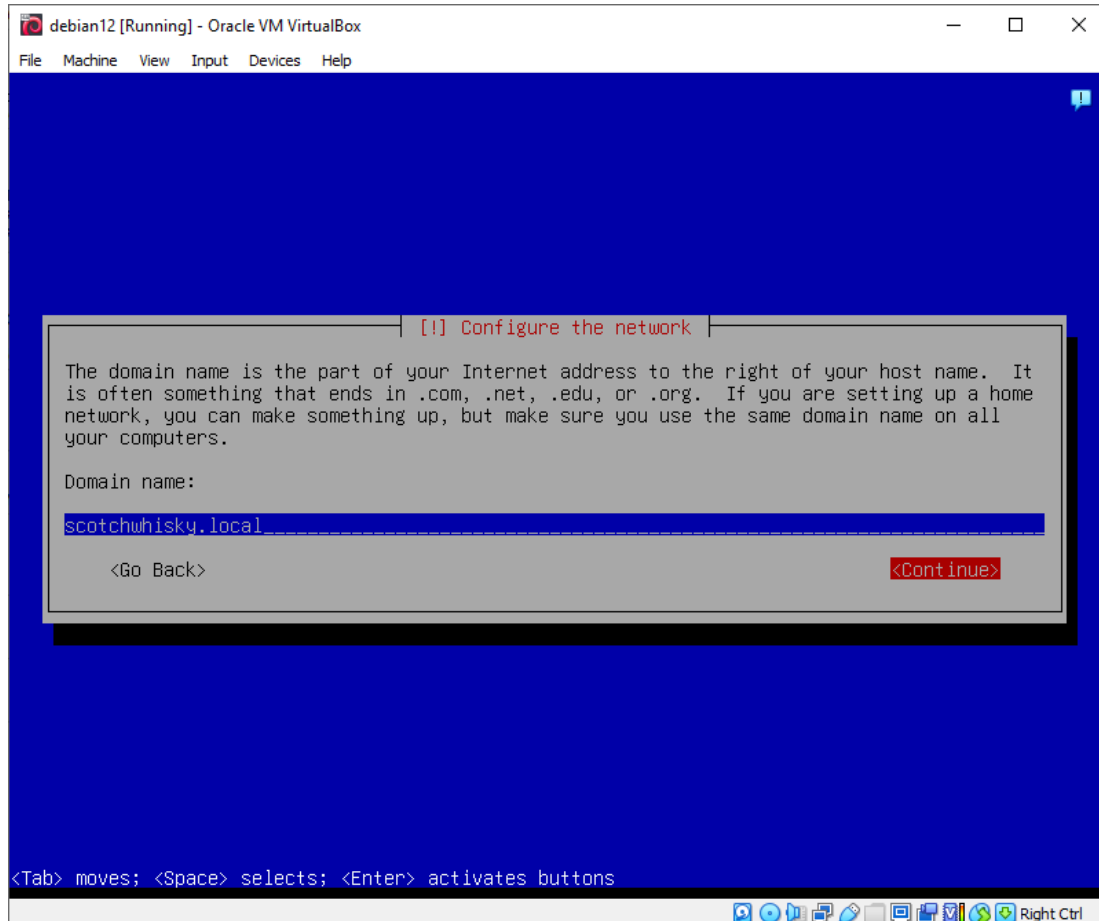




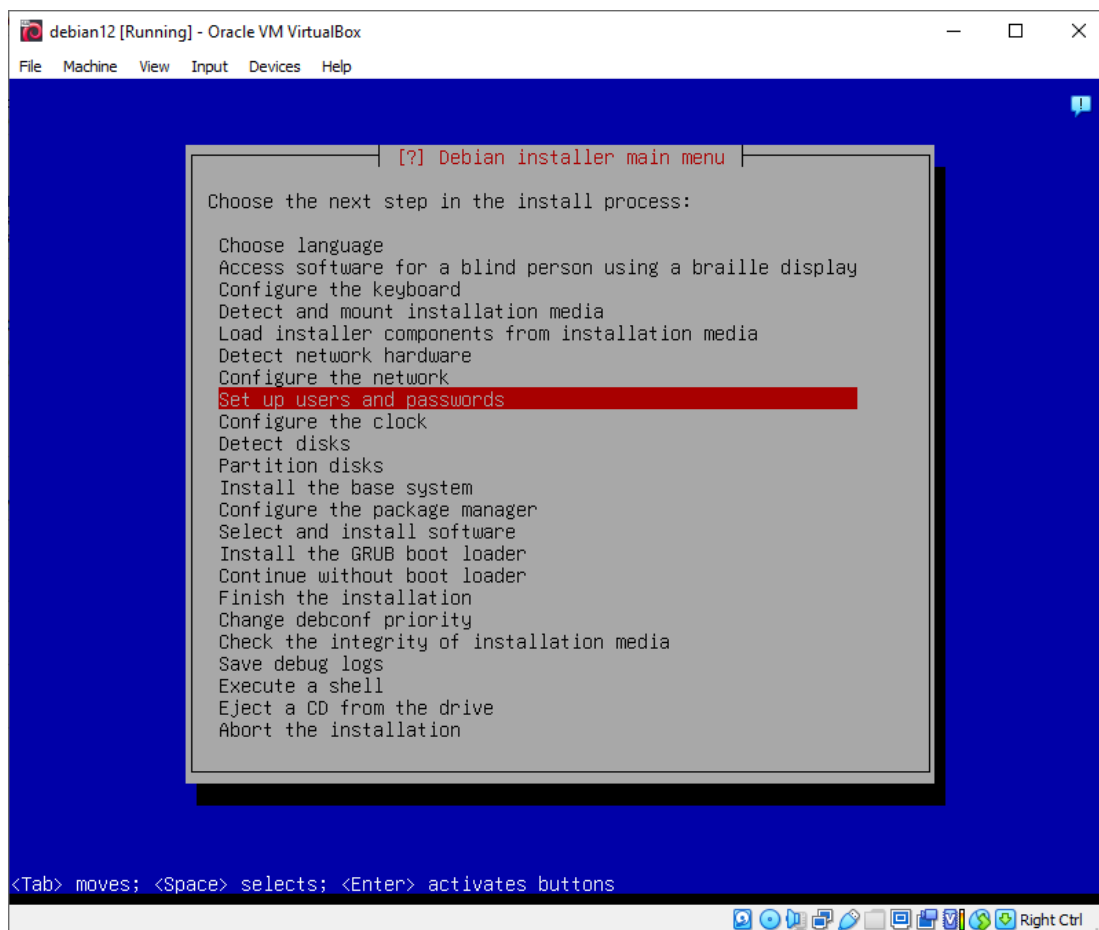
Set the hostname to your login suffixed by 42 e.g. pete42



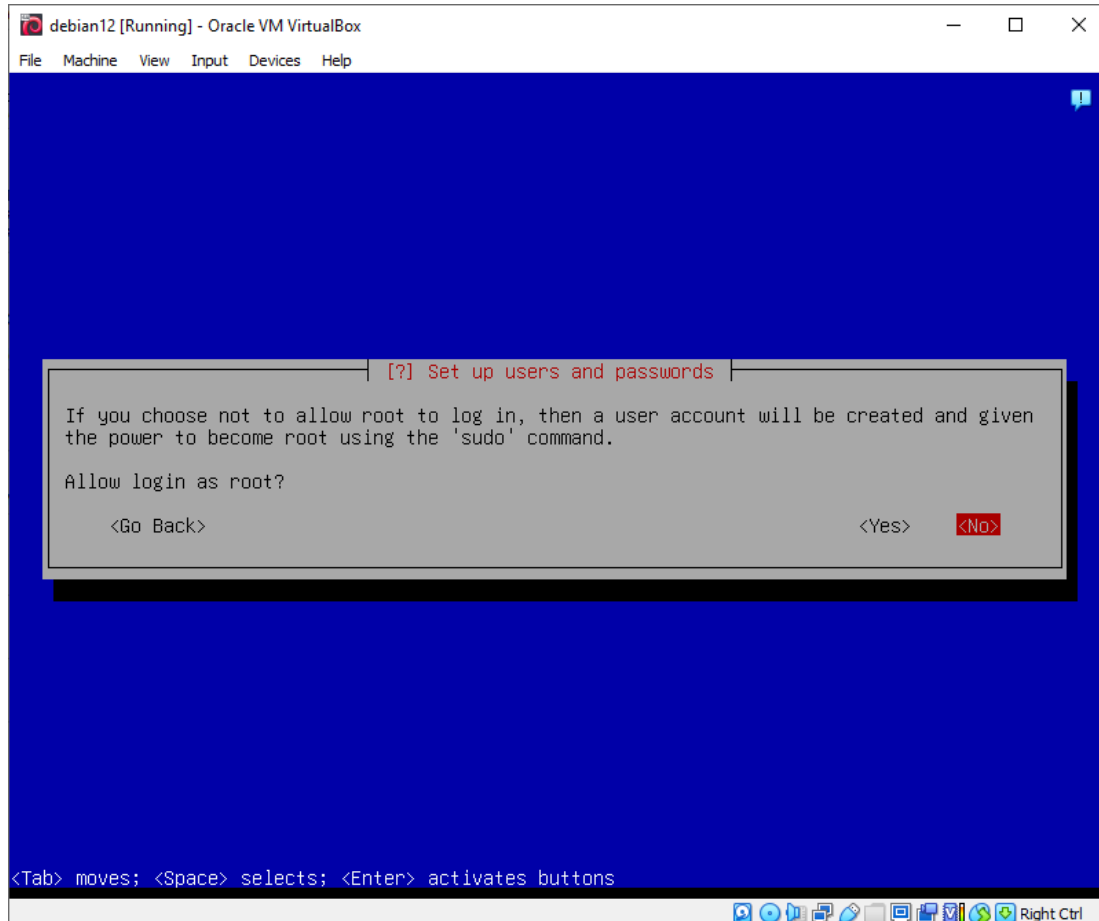
Nothing in documentation about the domain name so I used the usual domain for my other VMs e.g. scotchwhisky.local

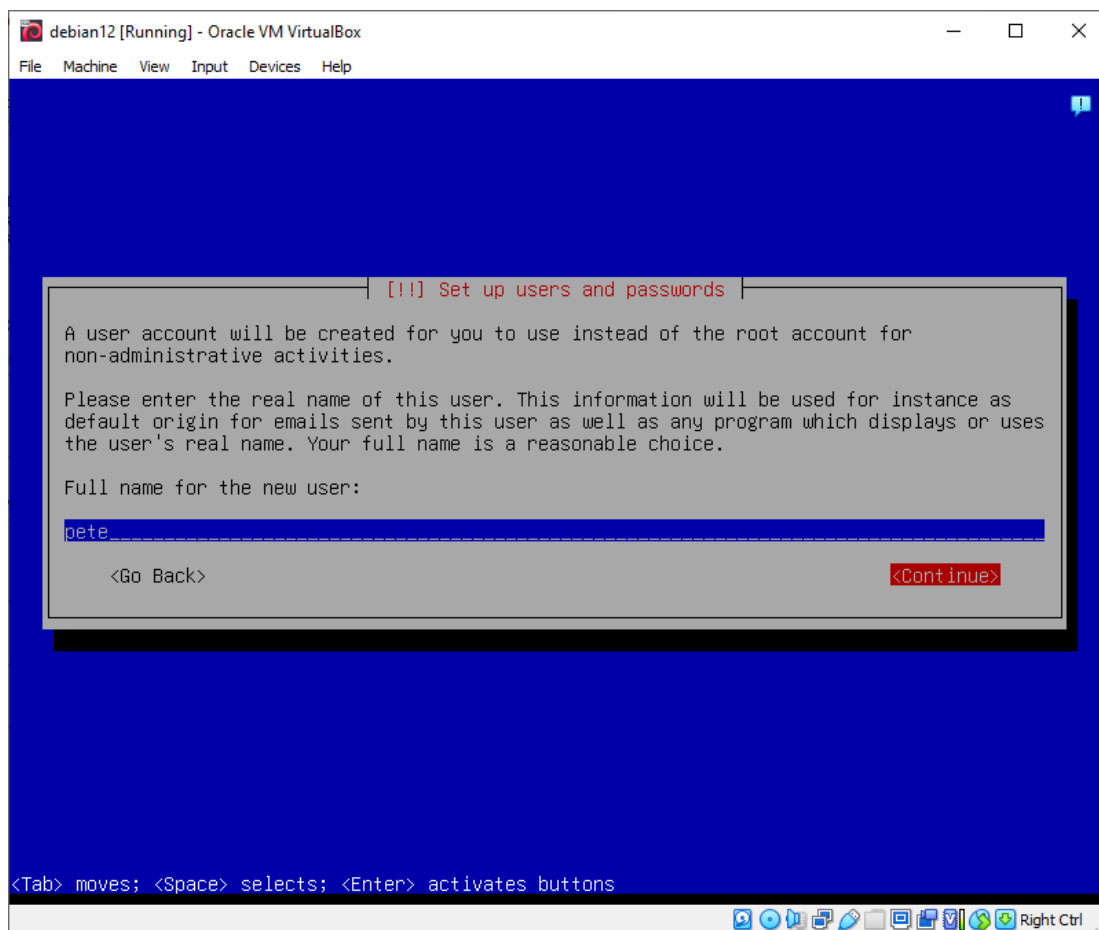




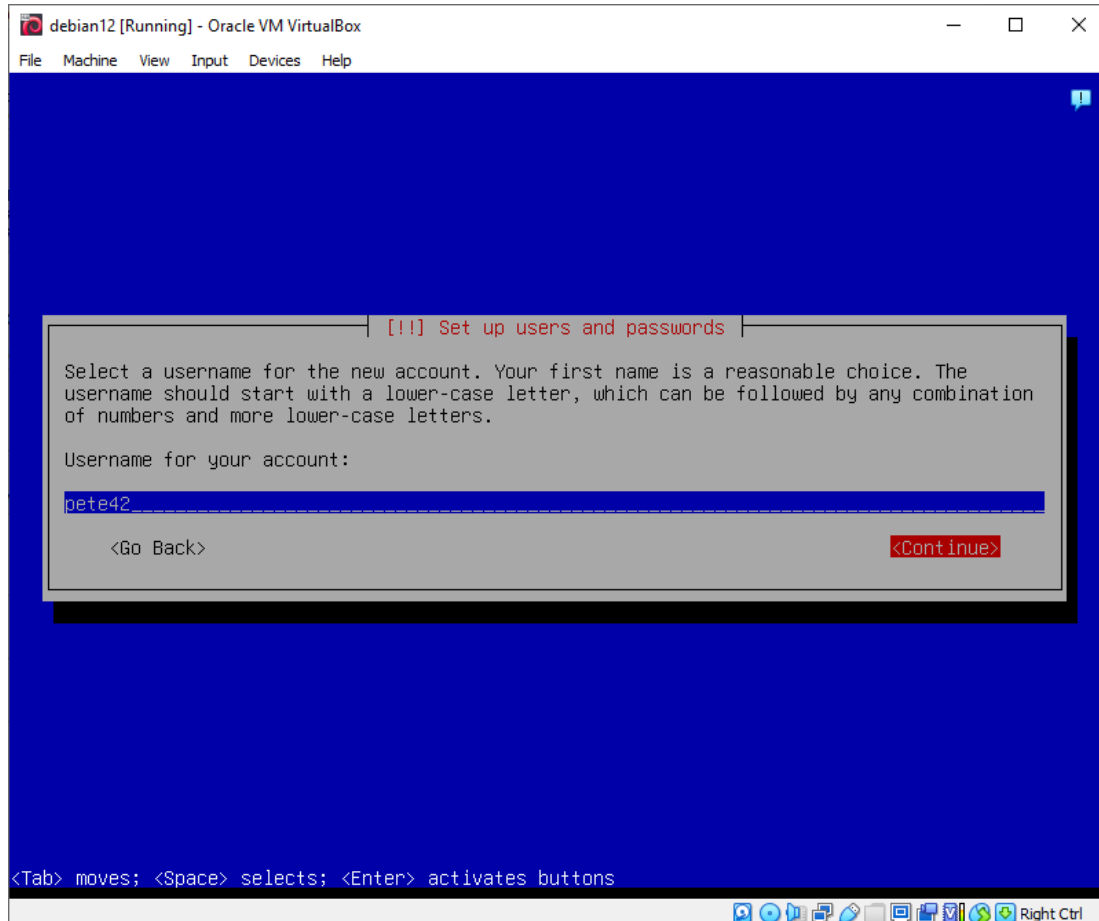


Don't allow root user login (uses sudo instead)

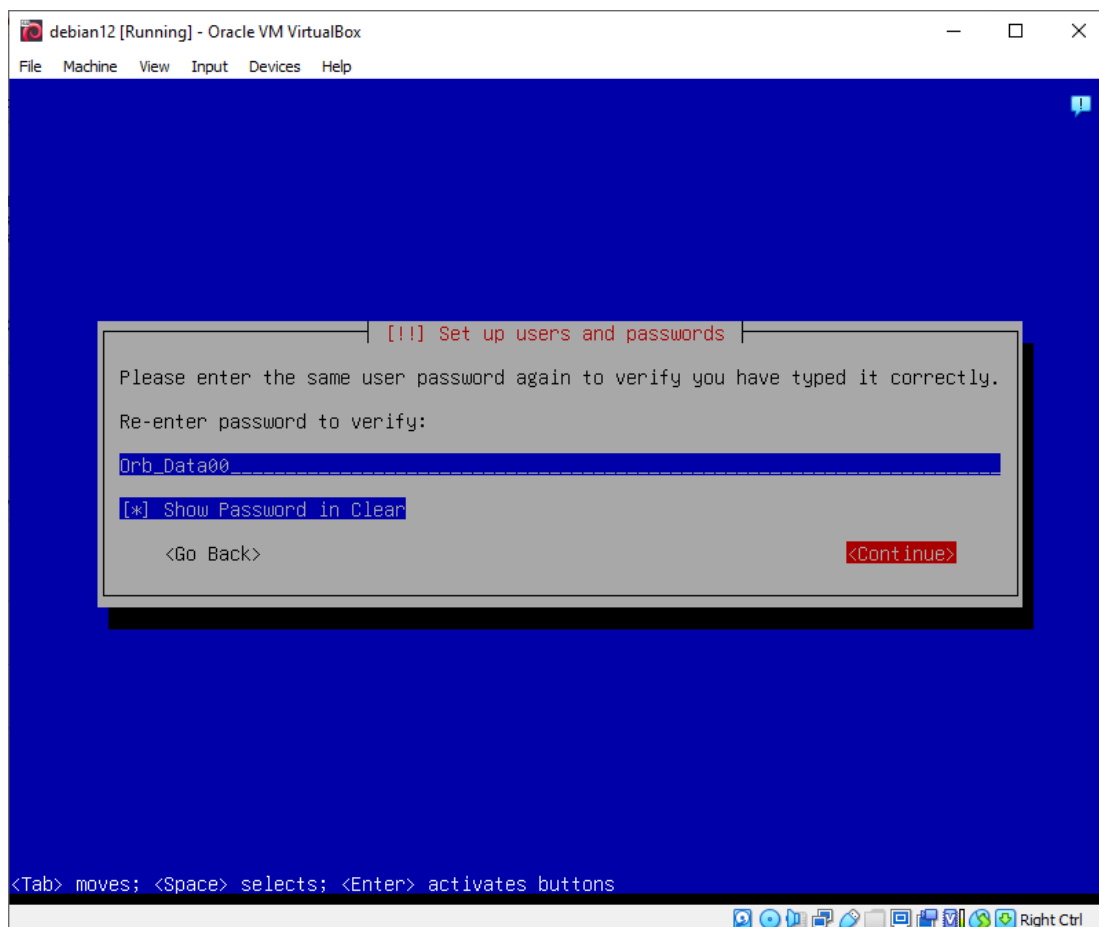
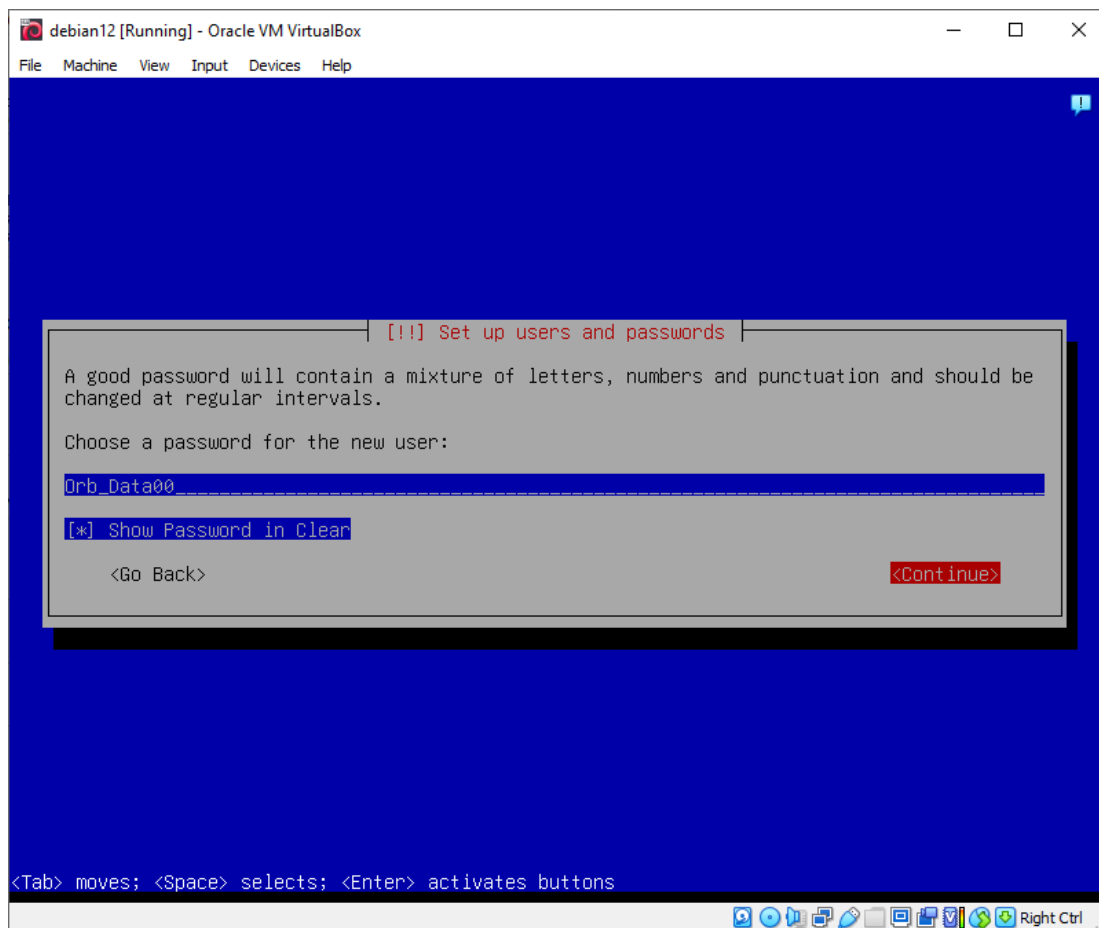


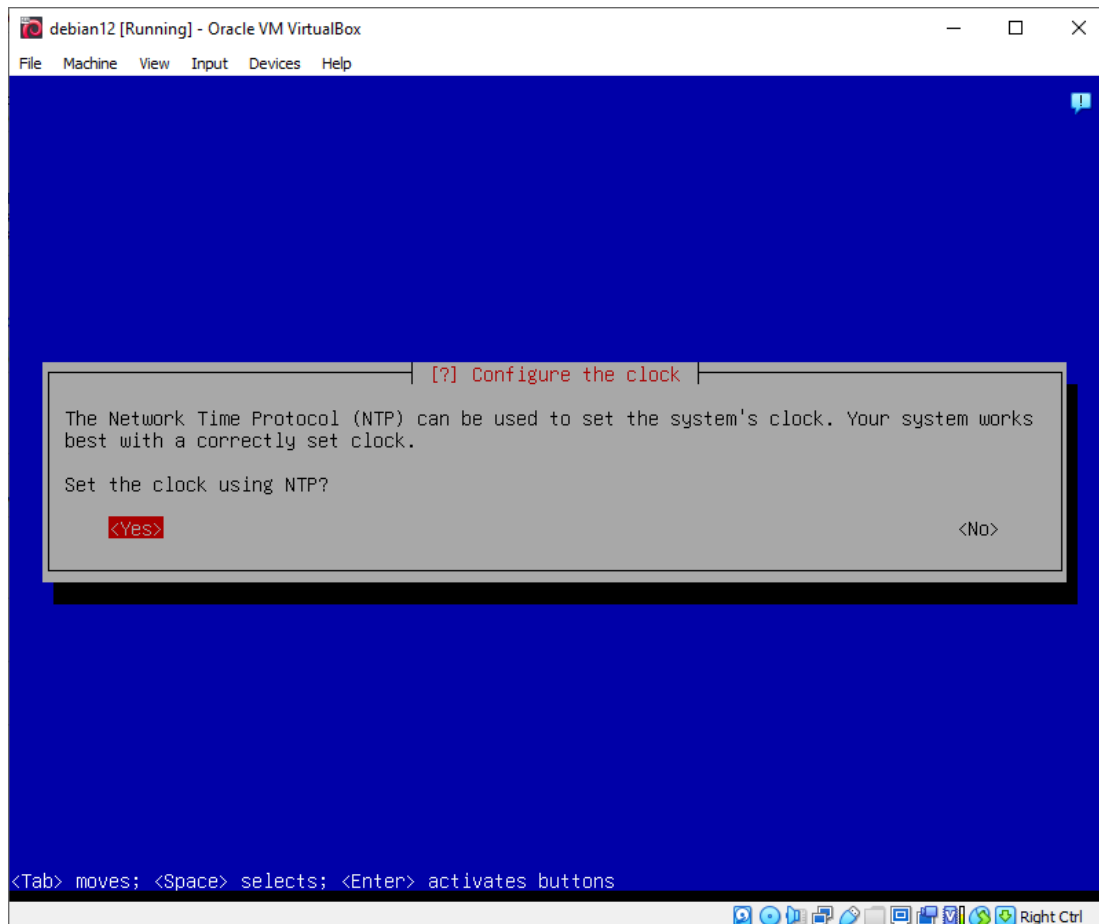
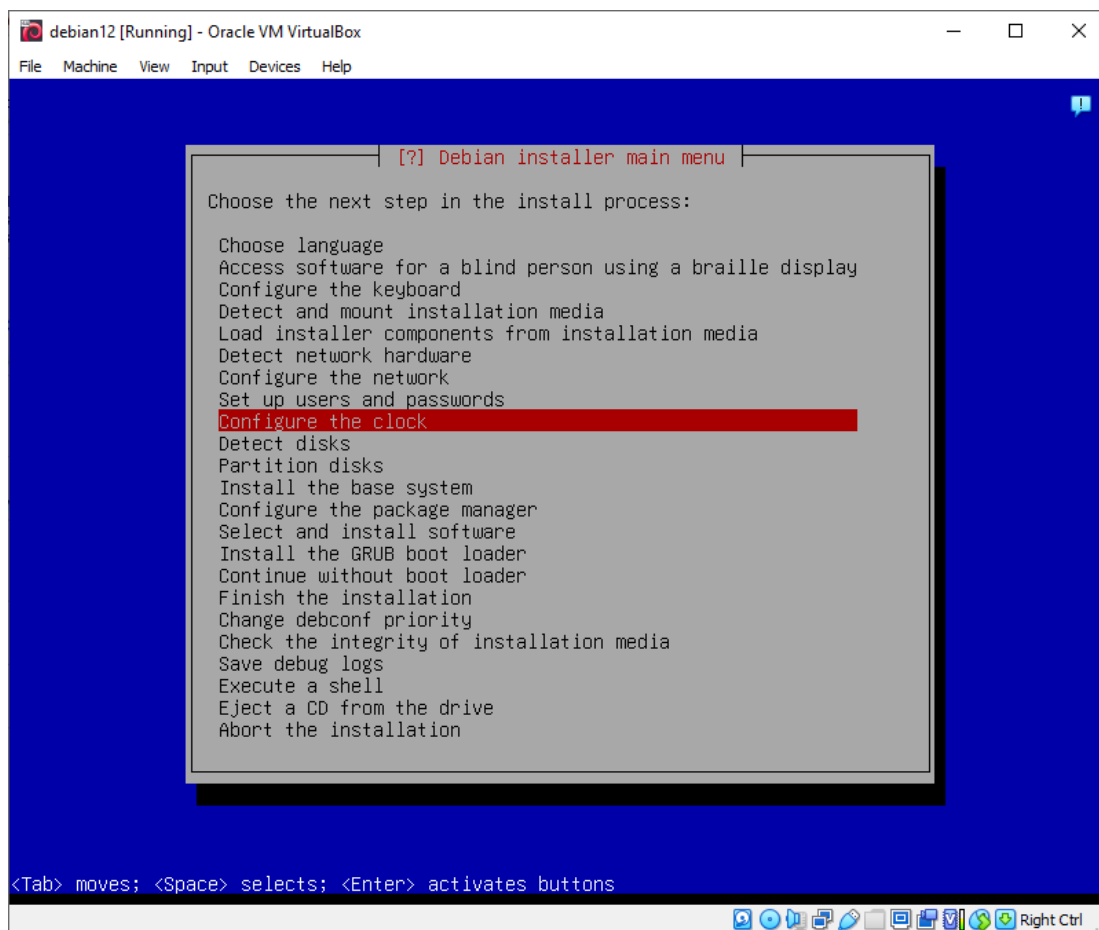


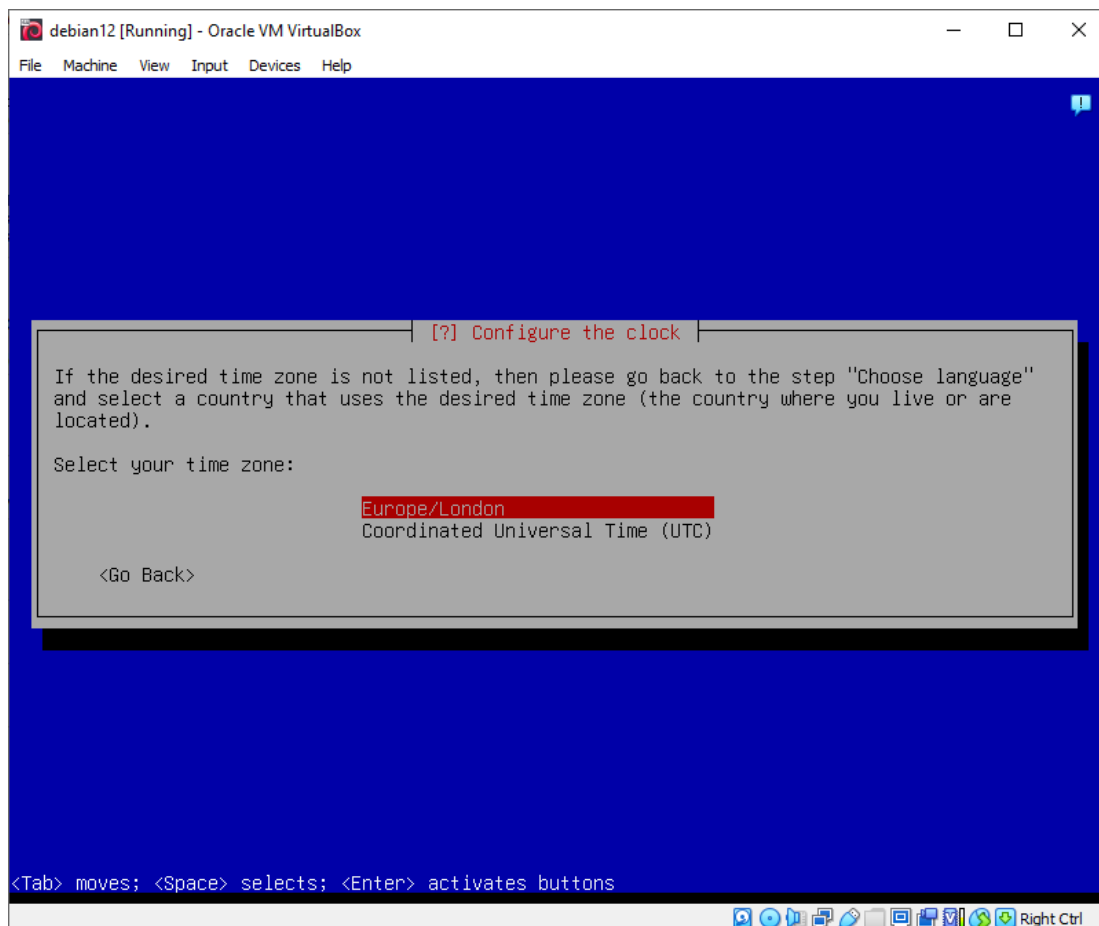
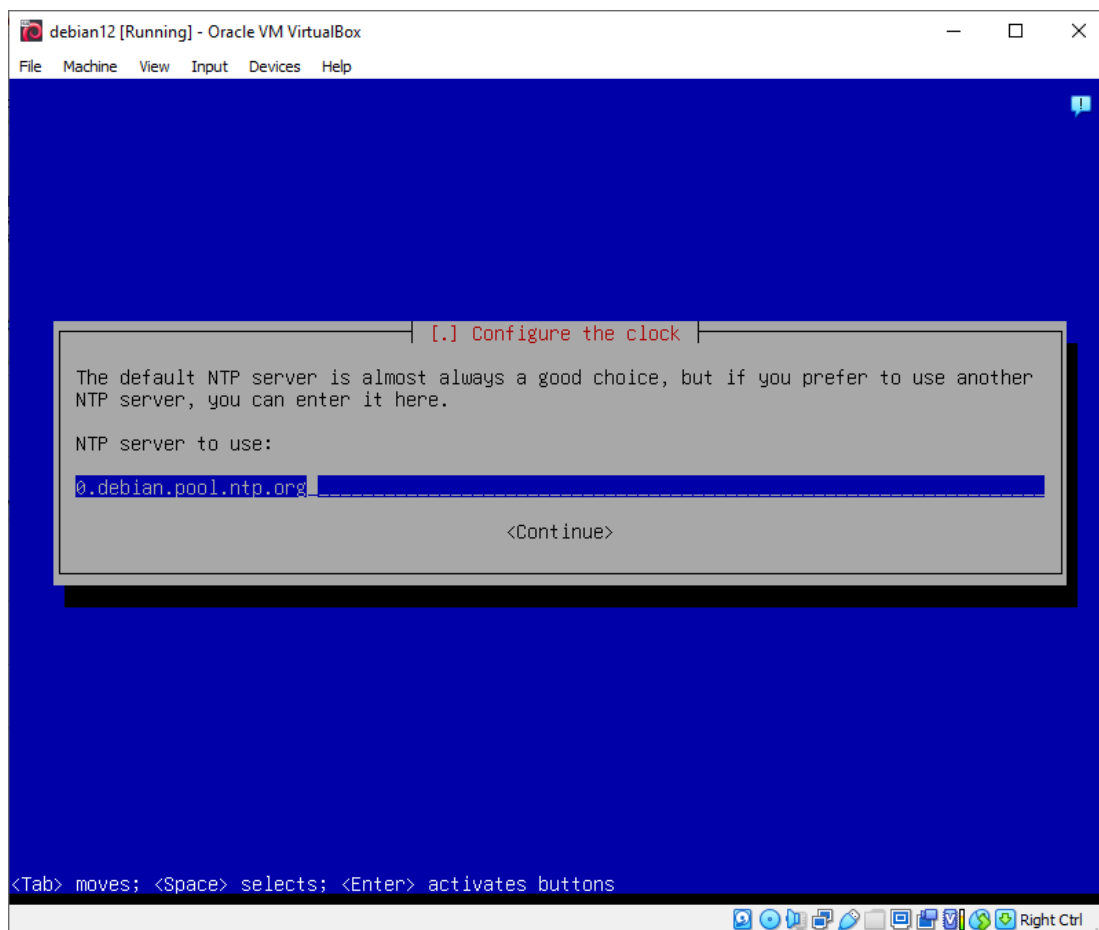
Set login to your login with "42" e.g. pete42

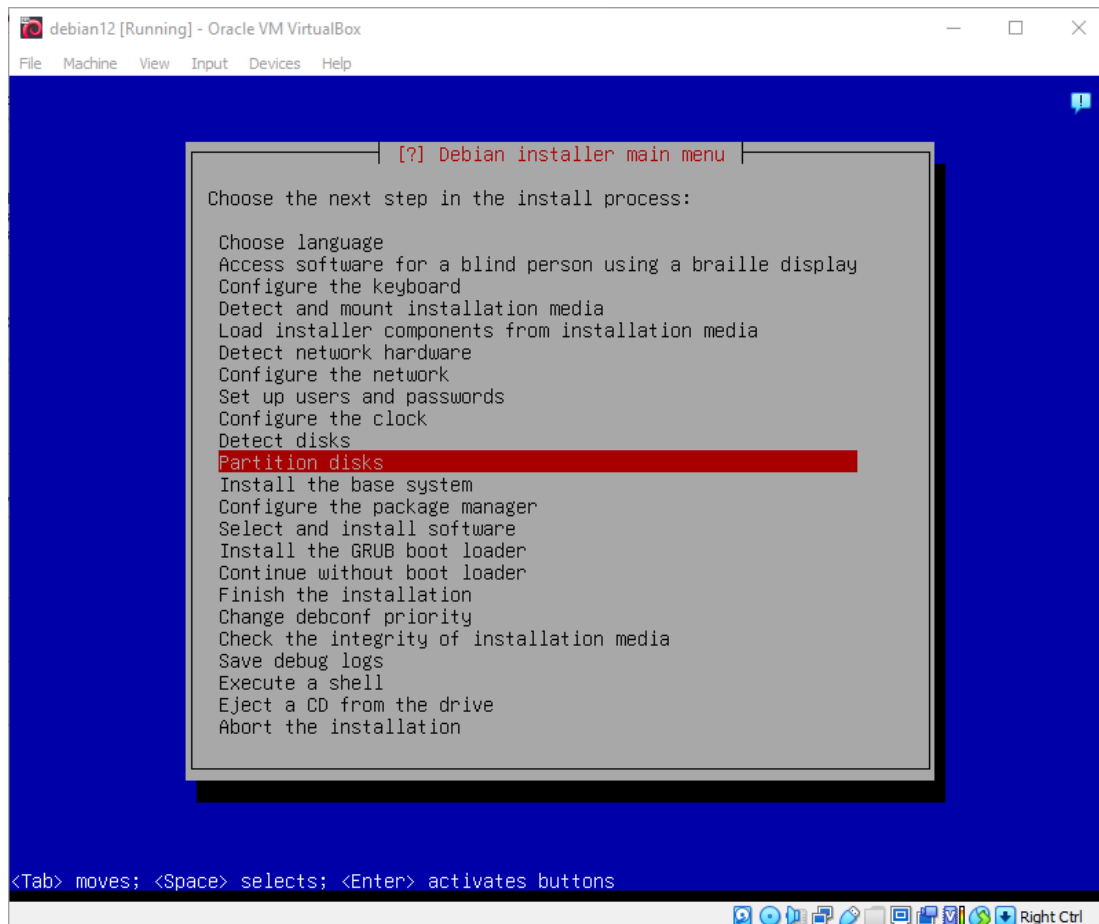
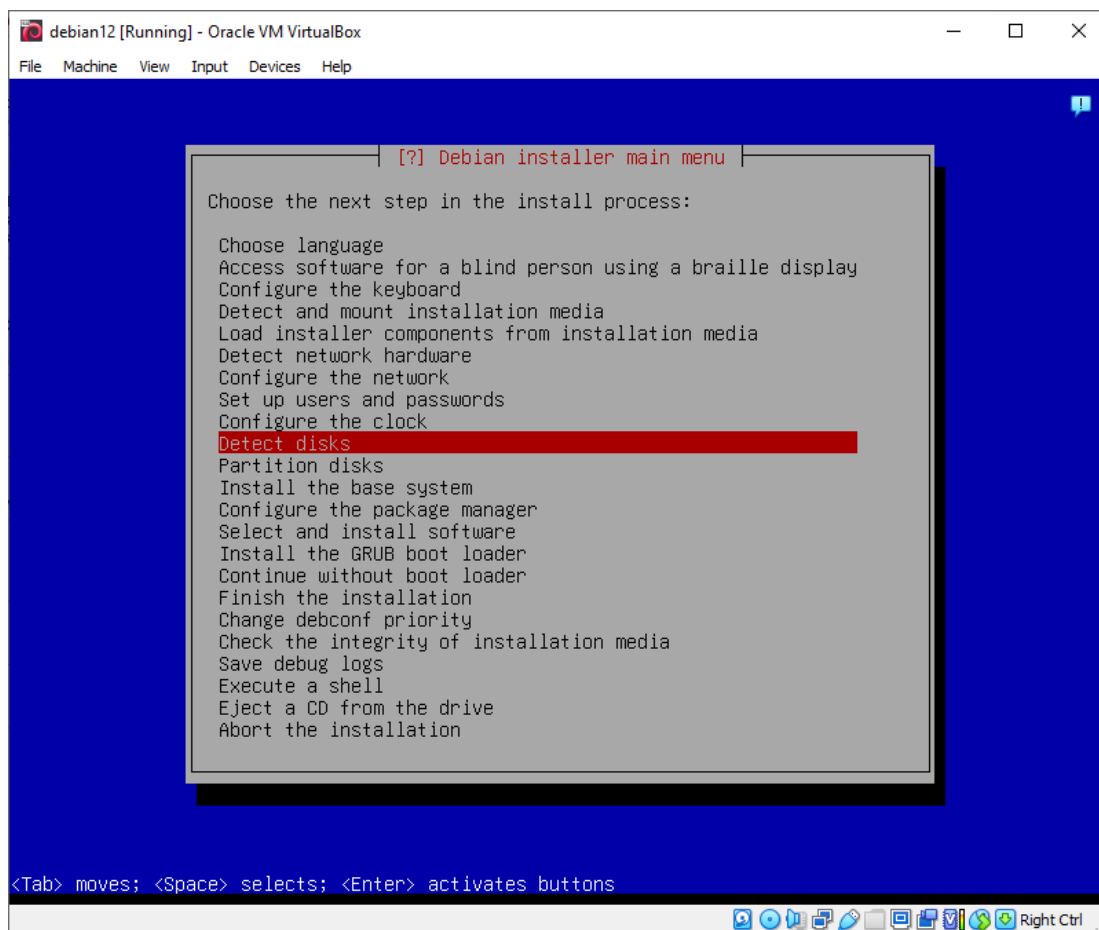


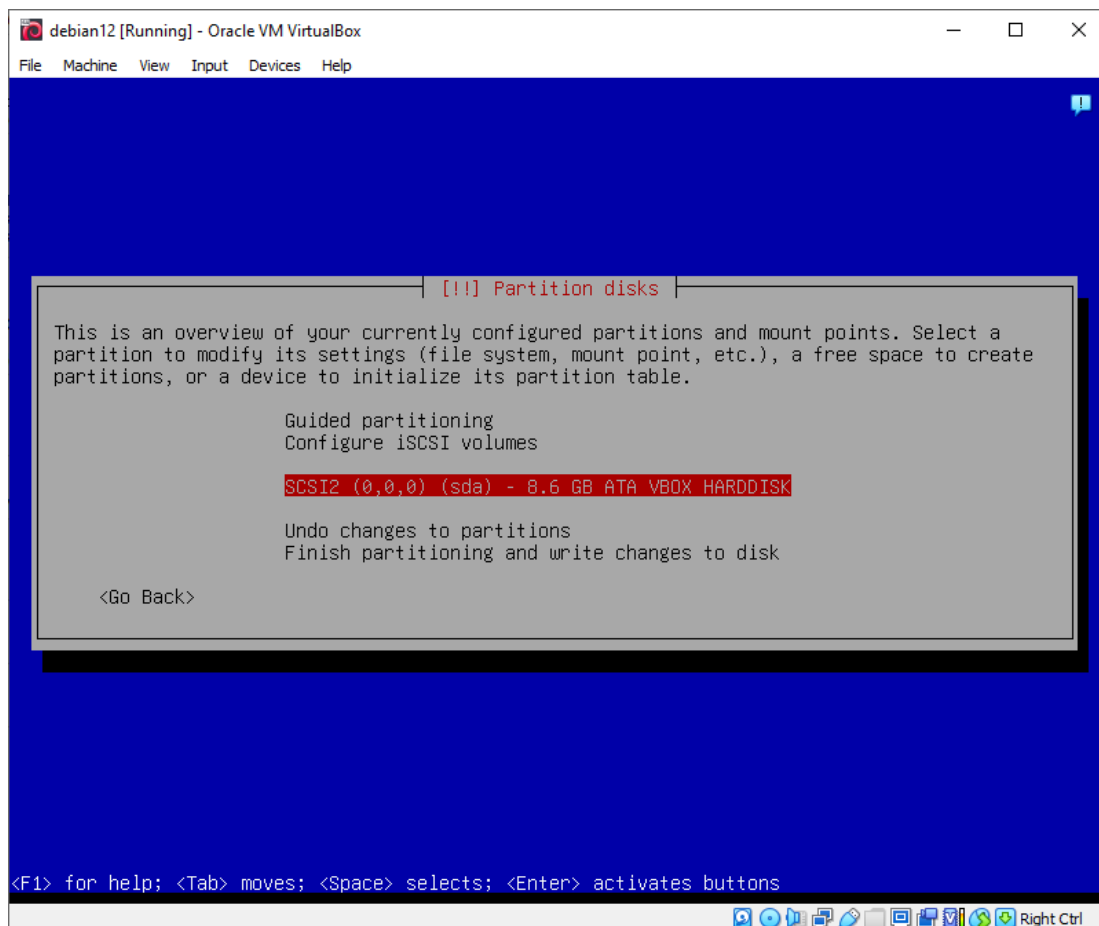
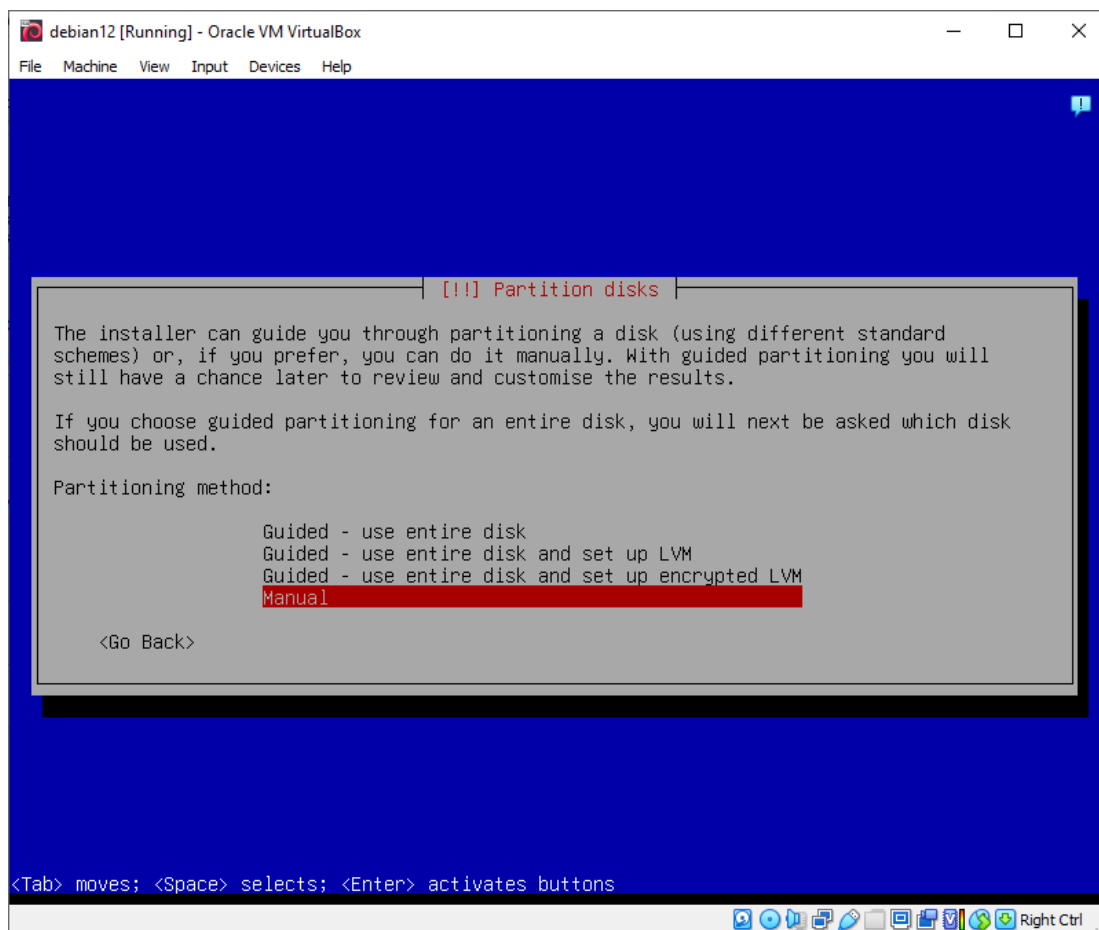
Set a minimum 10 character complex password as required by documentation

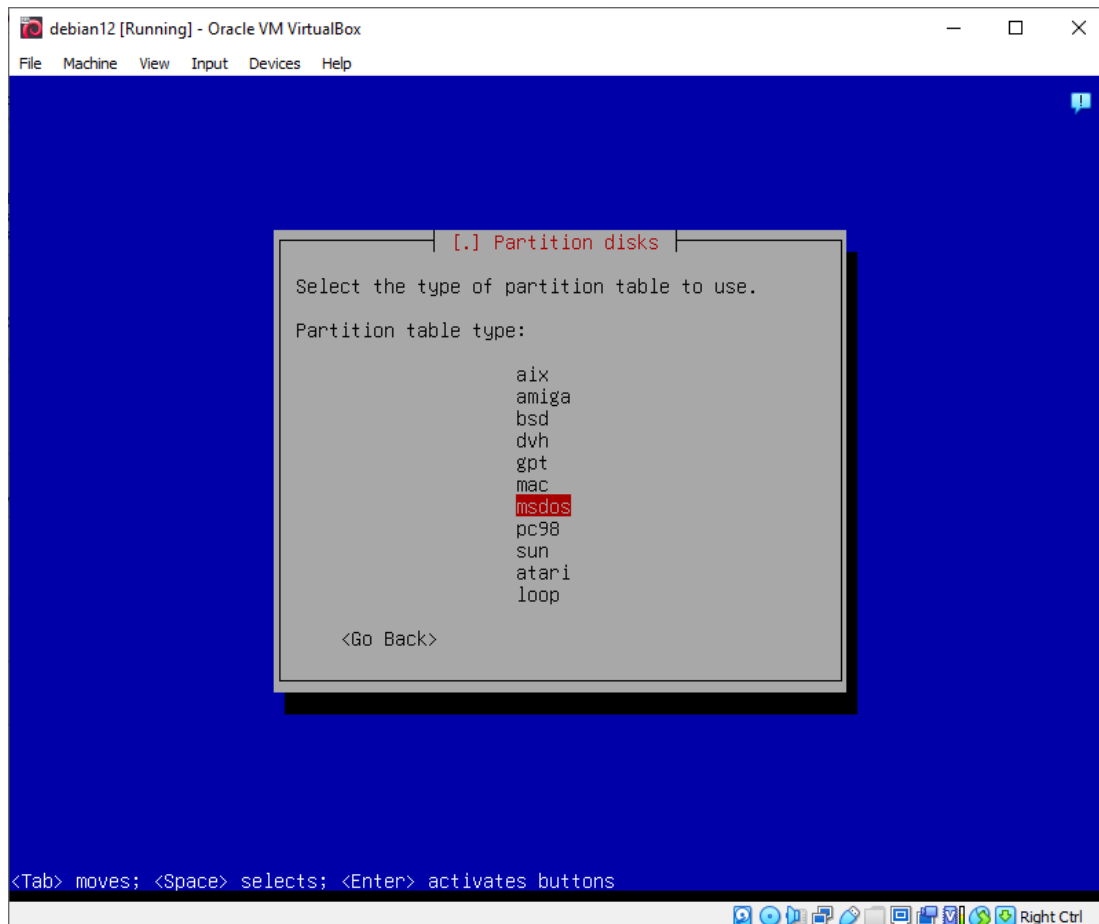
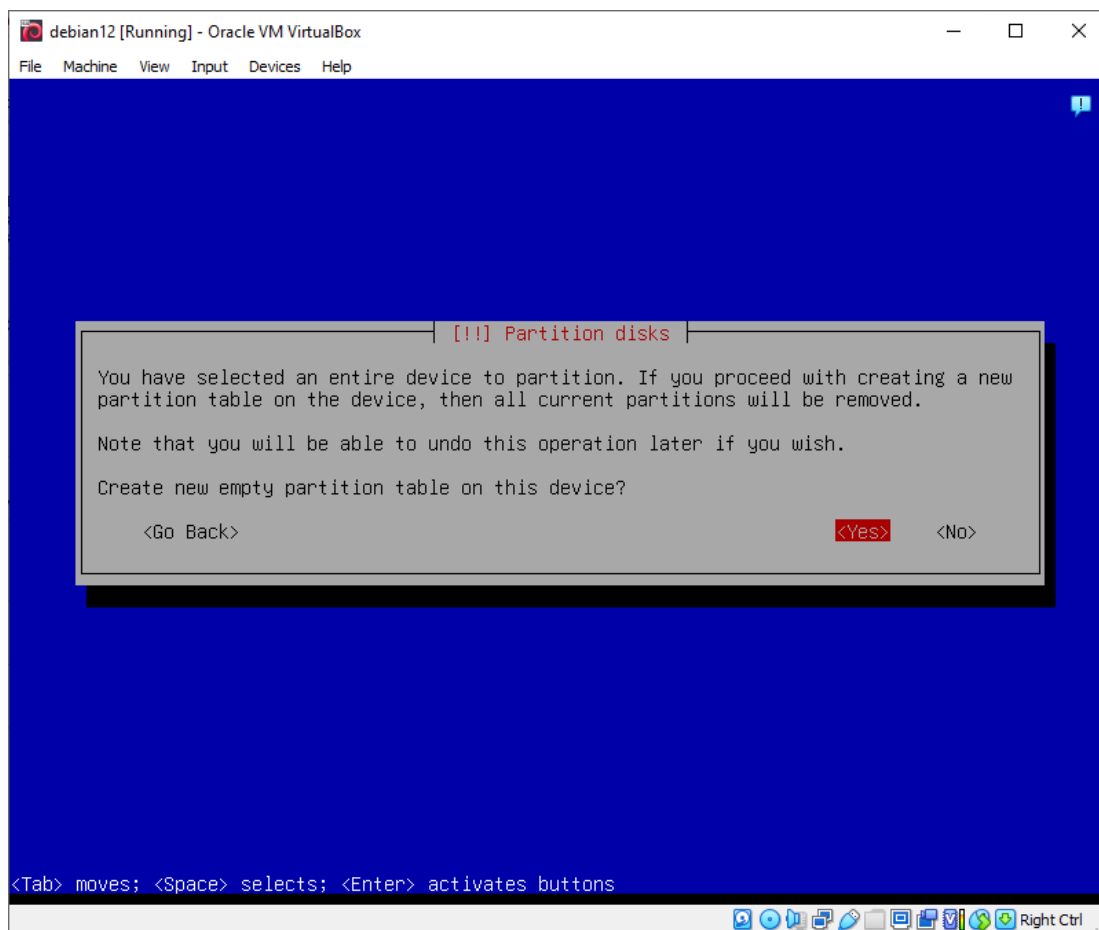




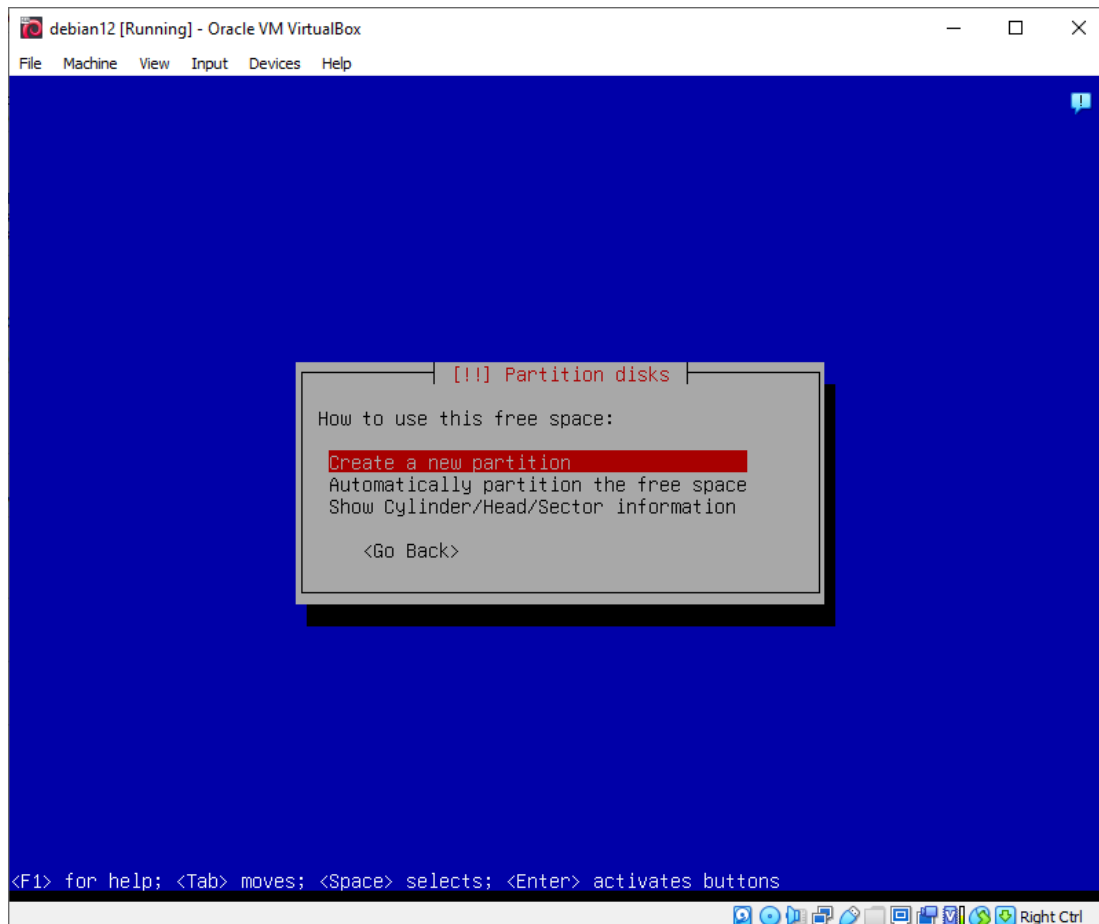
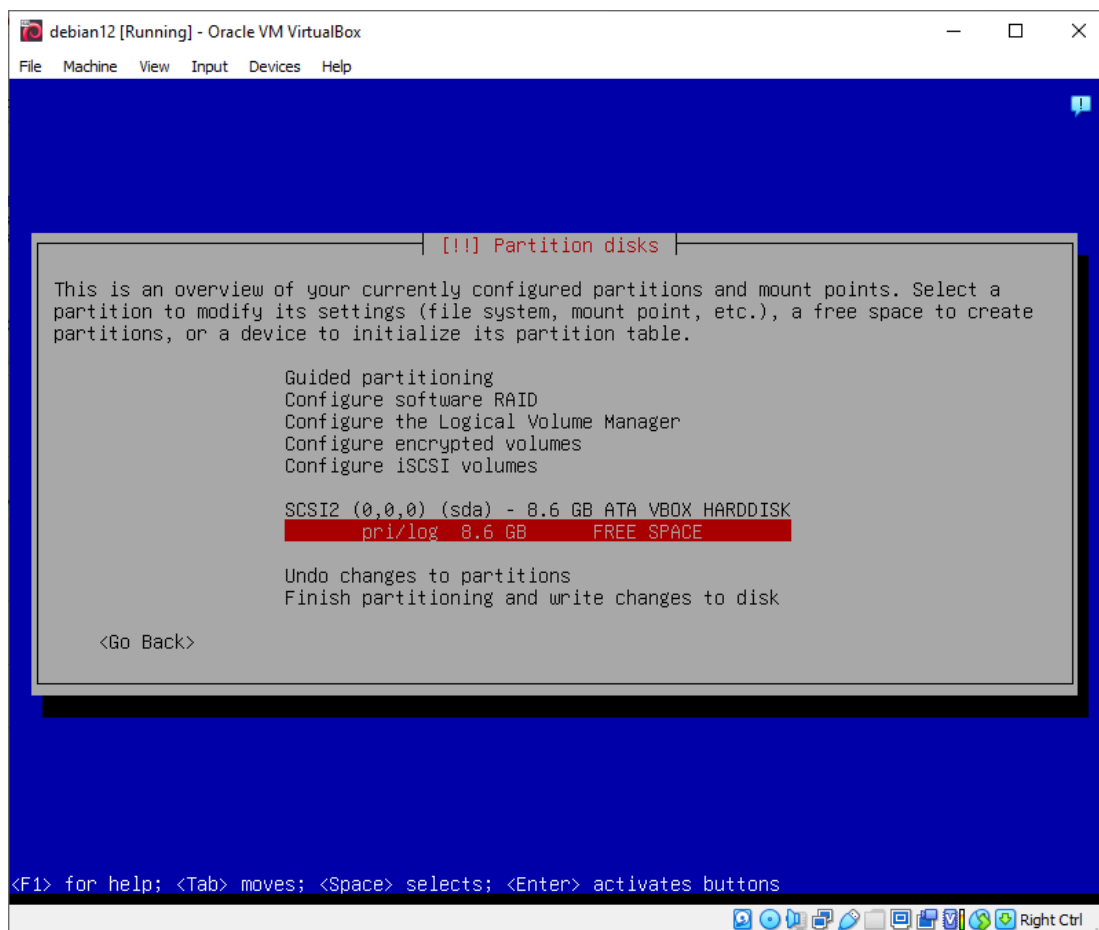


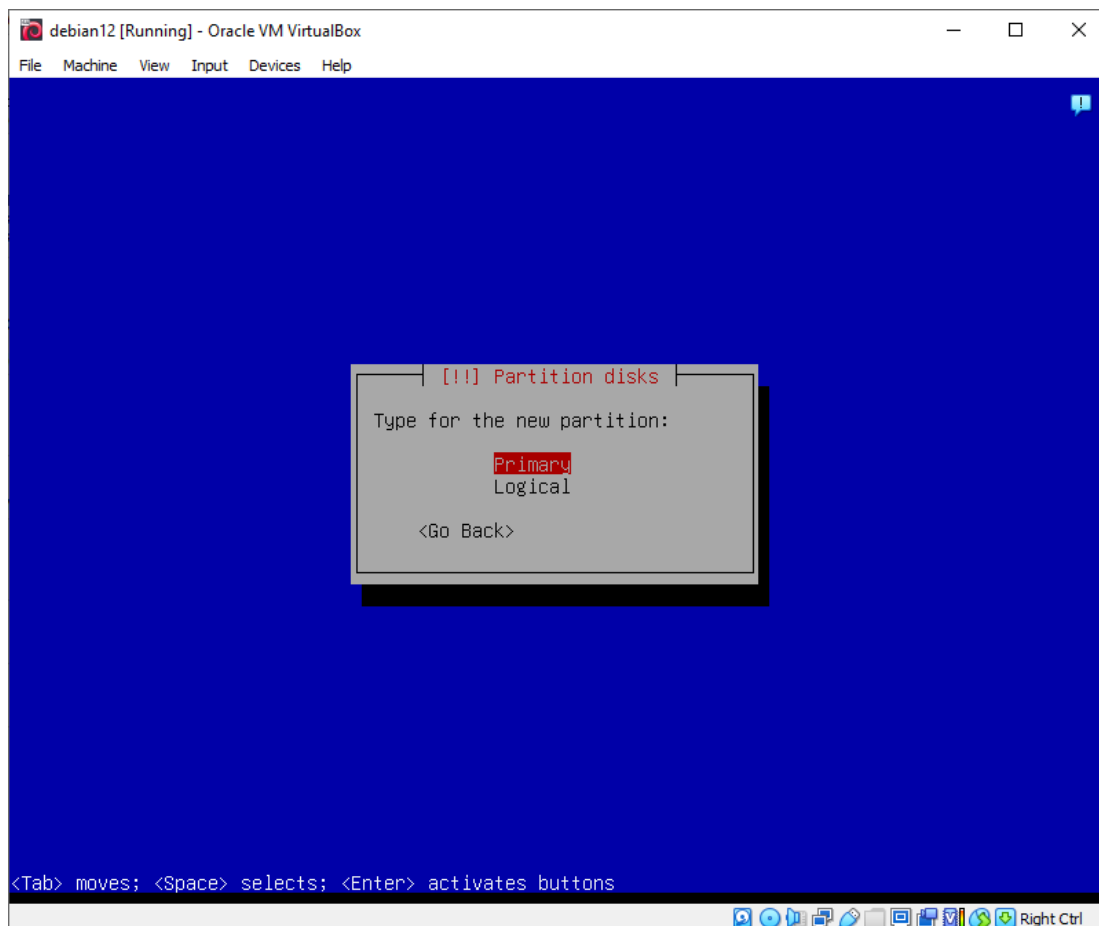
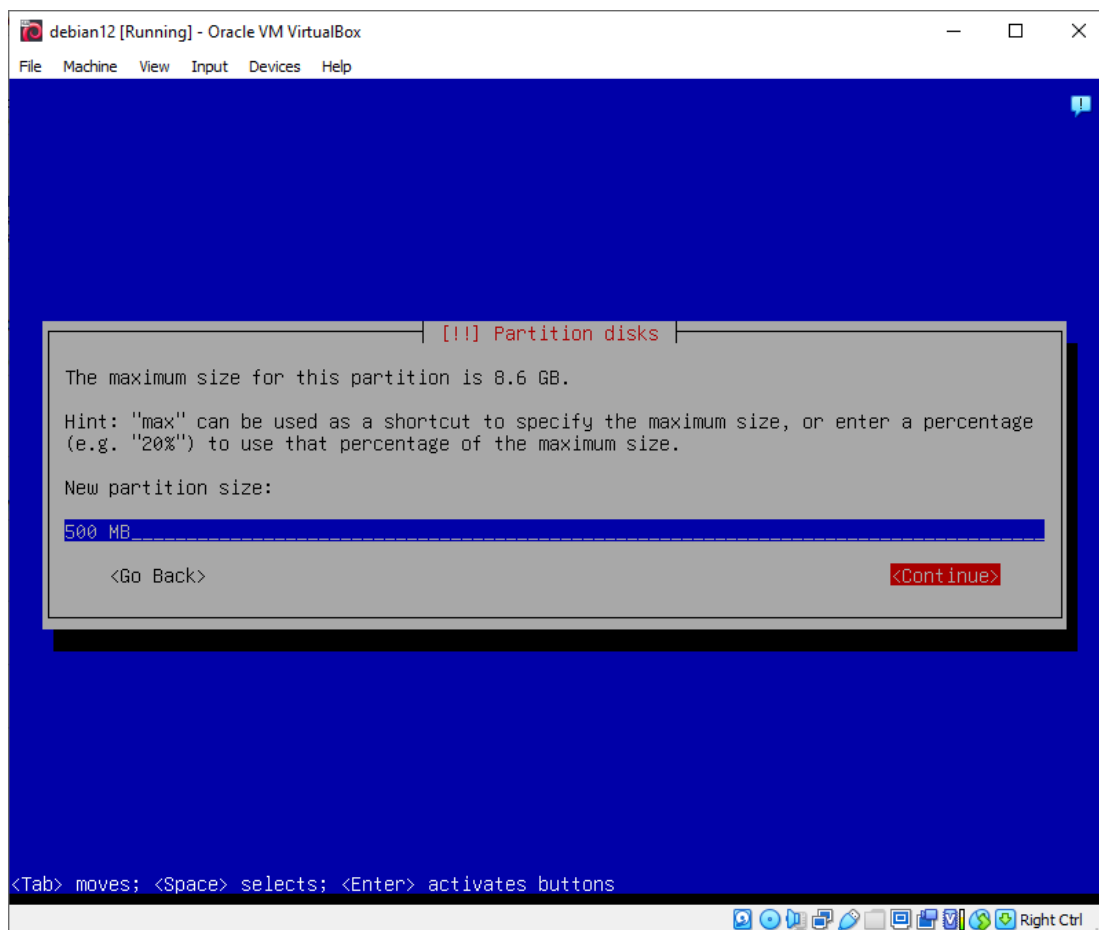


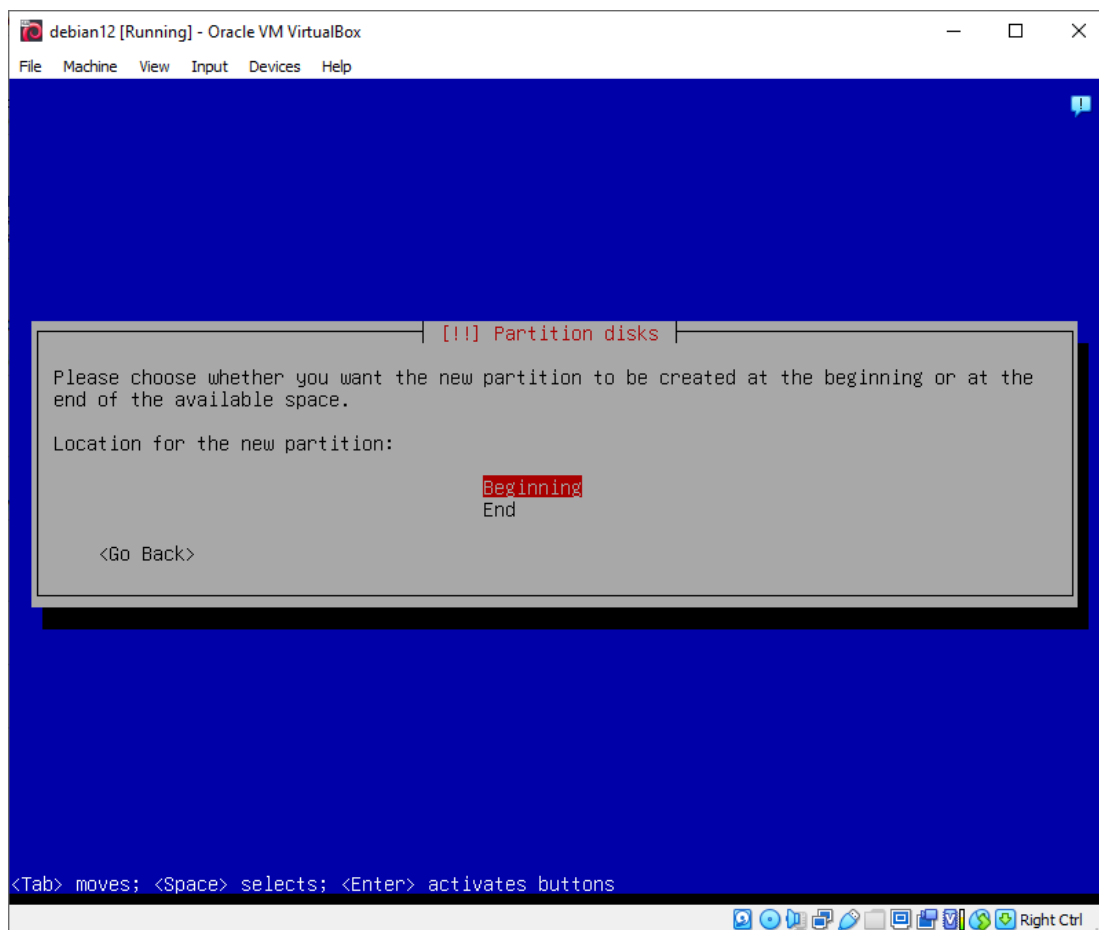




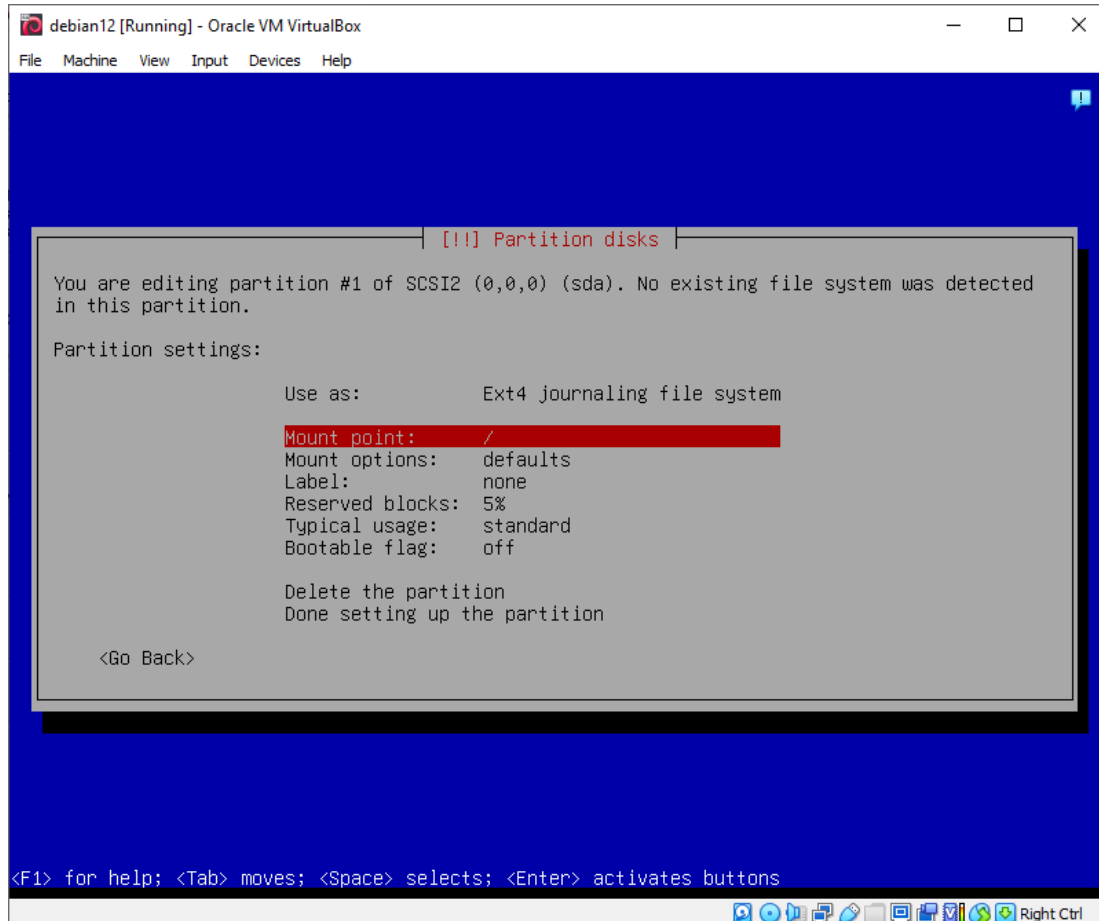




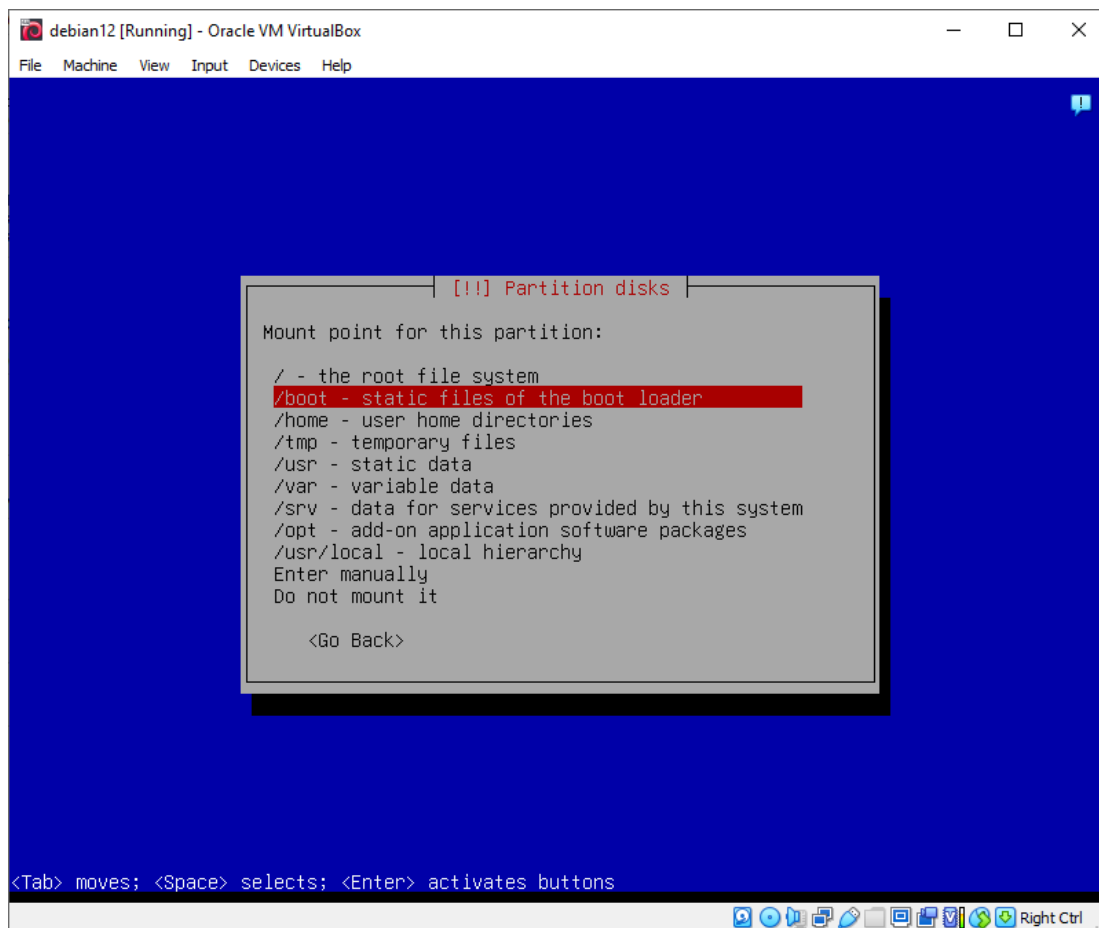




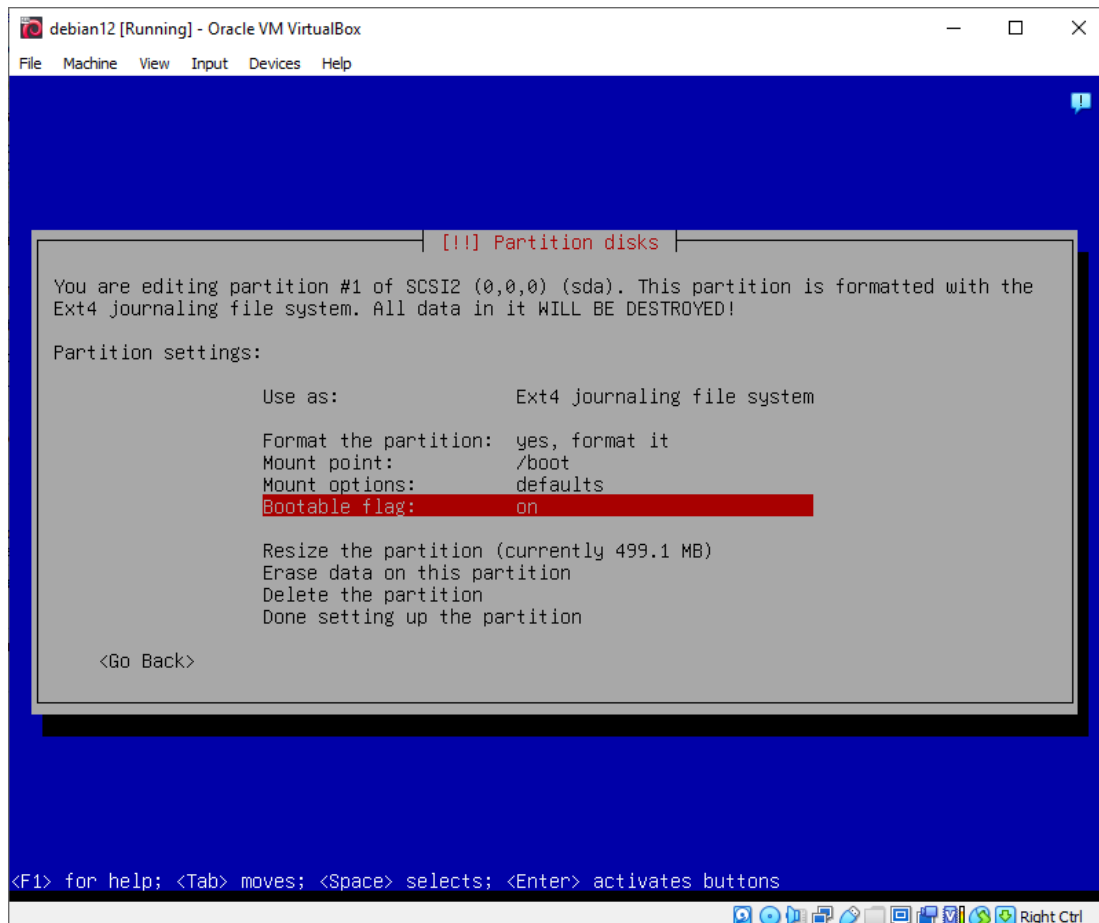
Select the Mount point and press enter



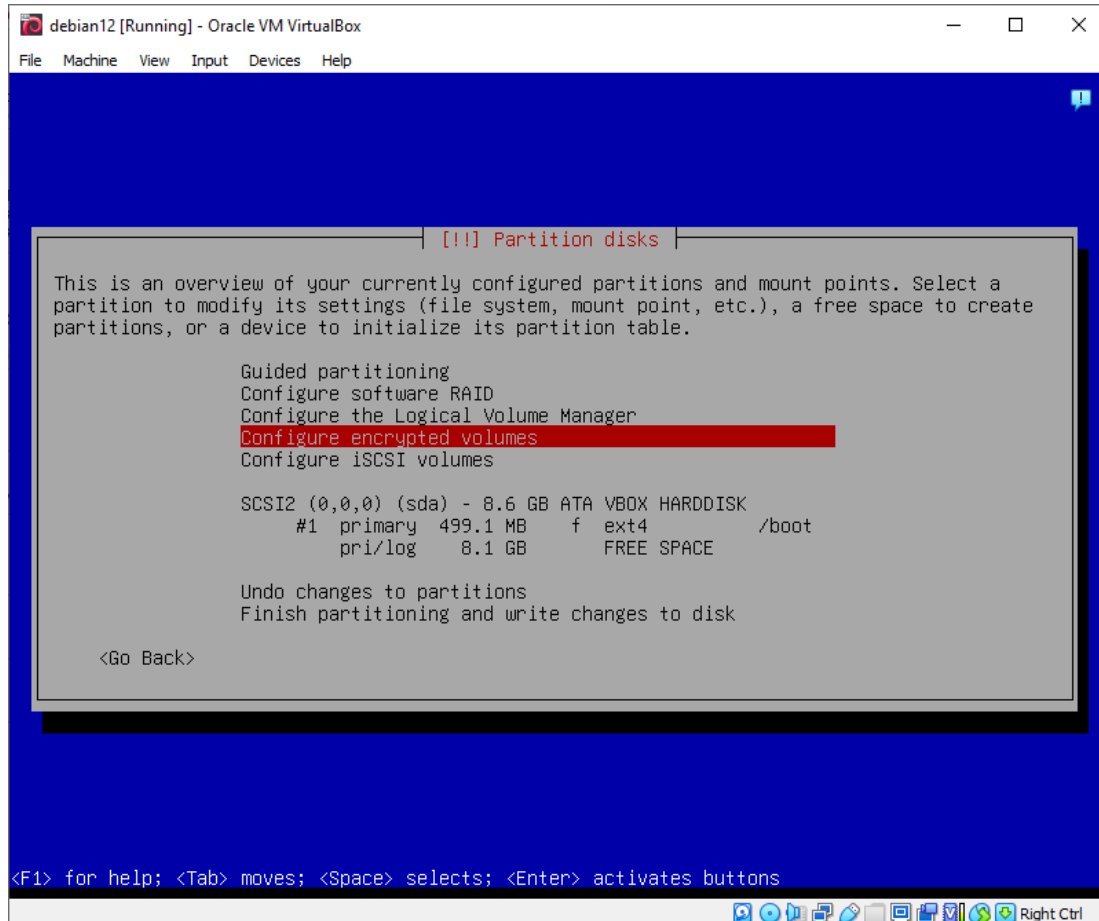
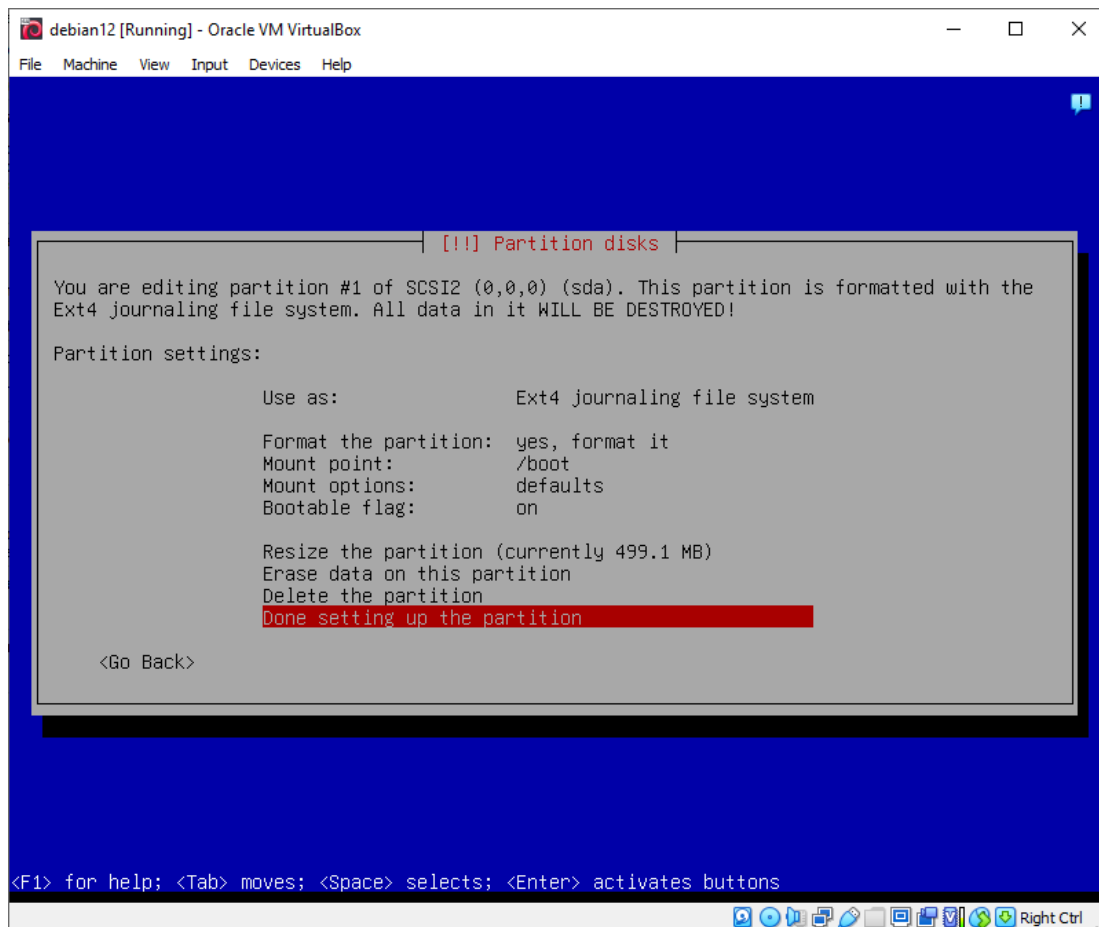
Select /boot and press enter

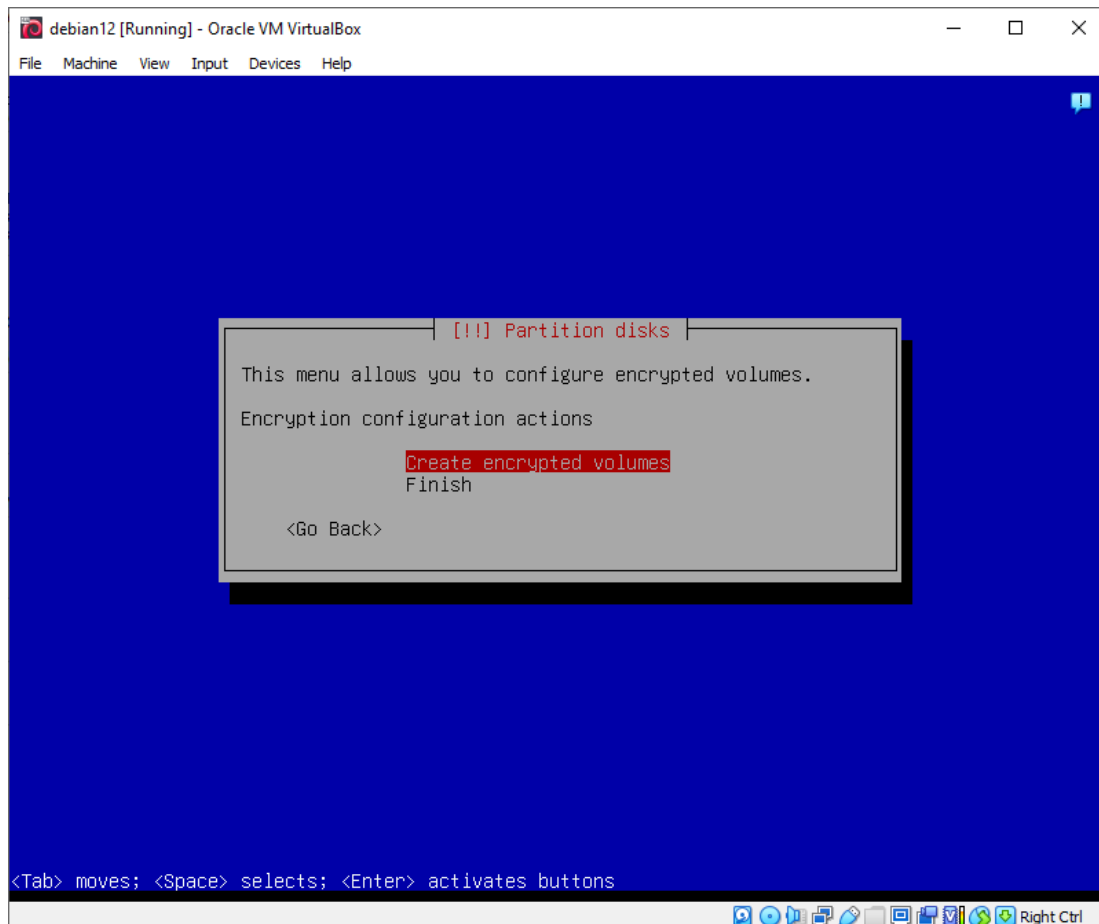
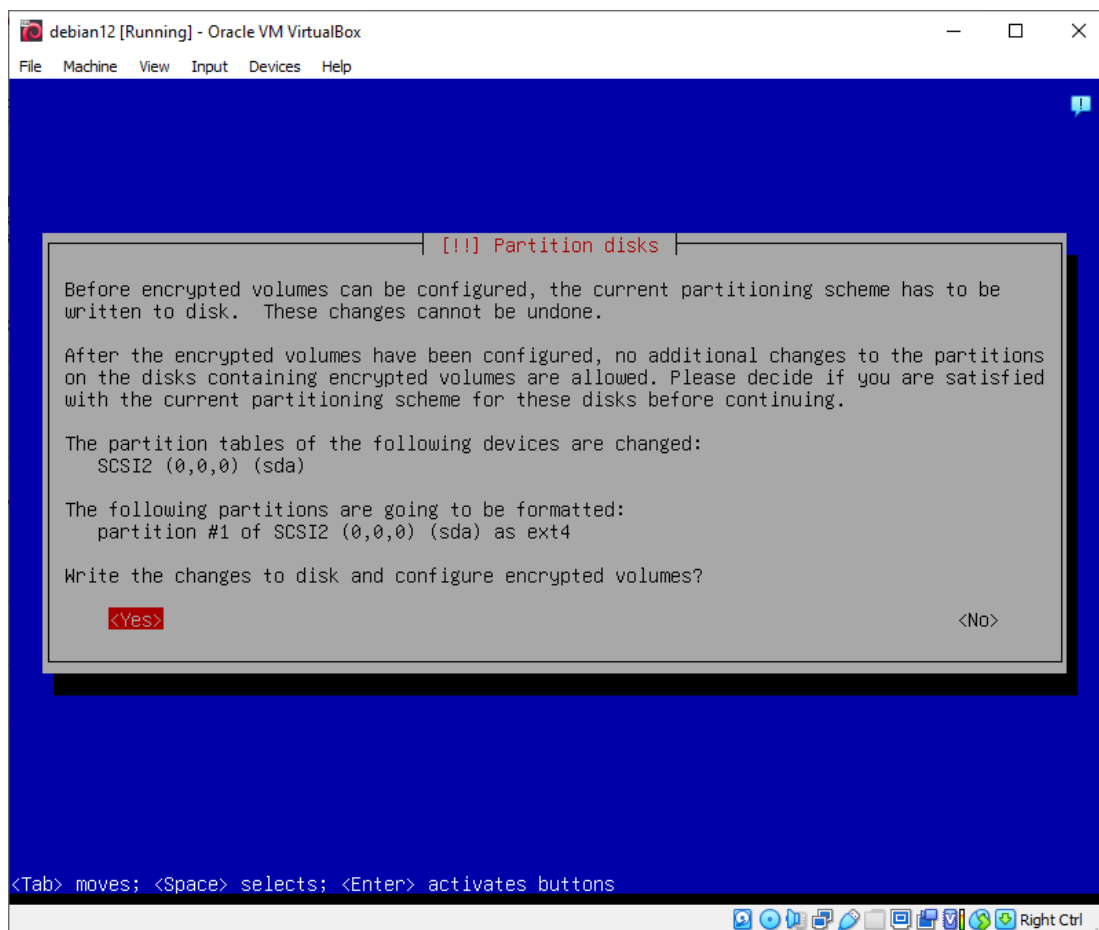


Select Bootable flag and press enter (makes partition bootable)

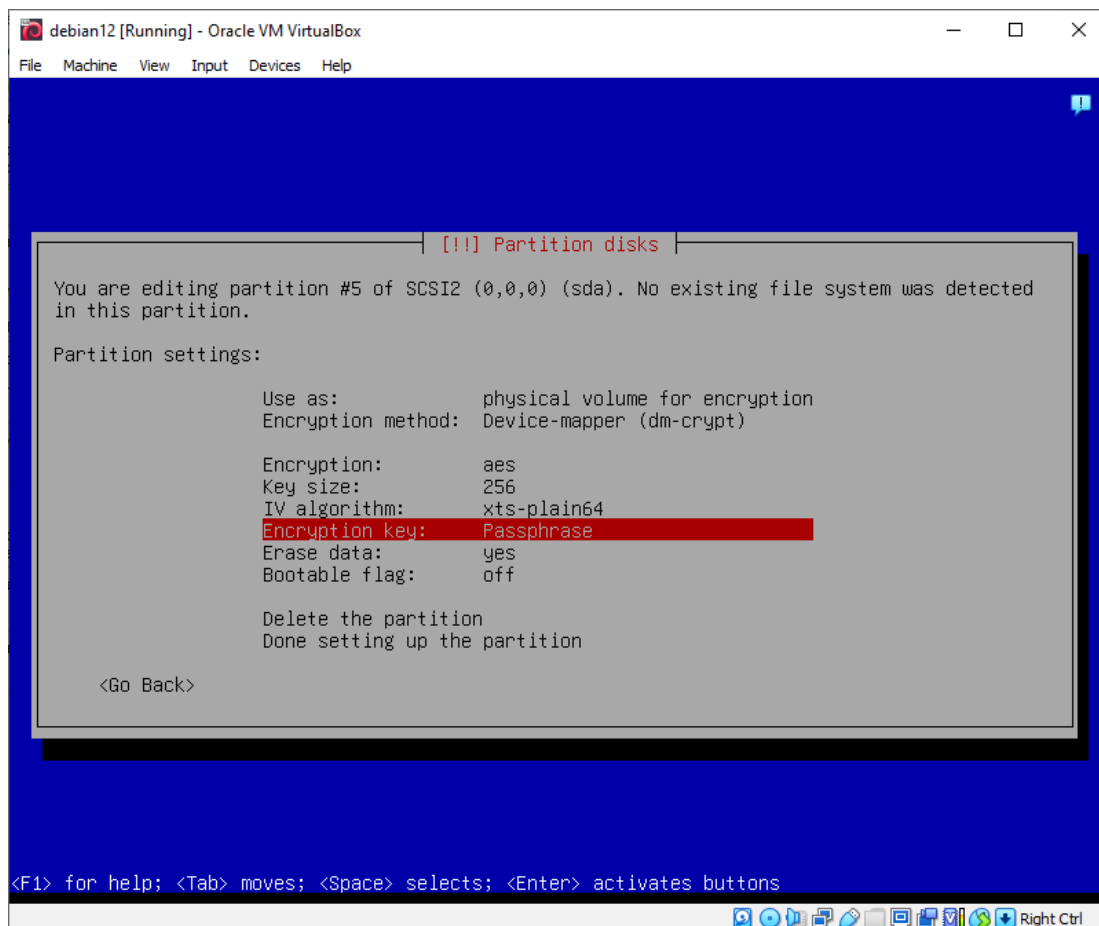
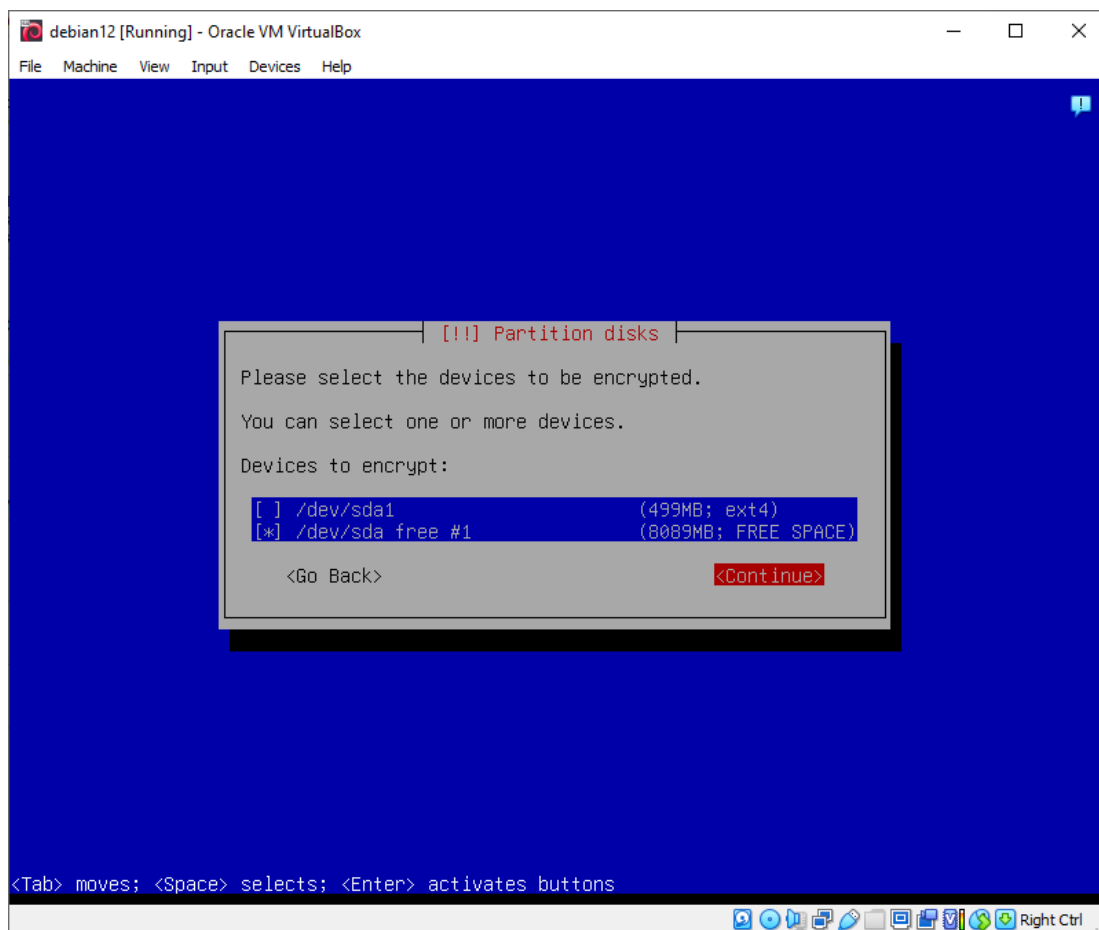


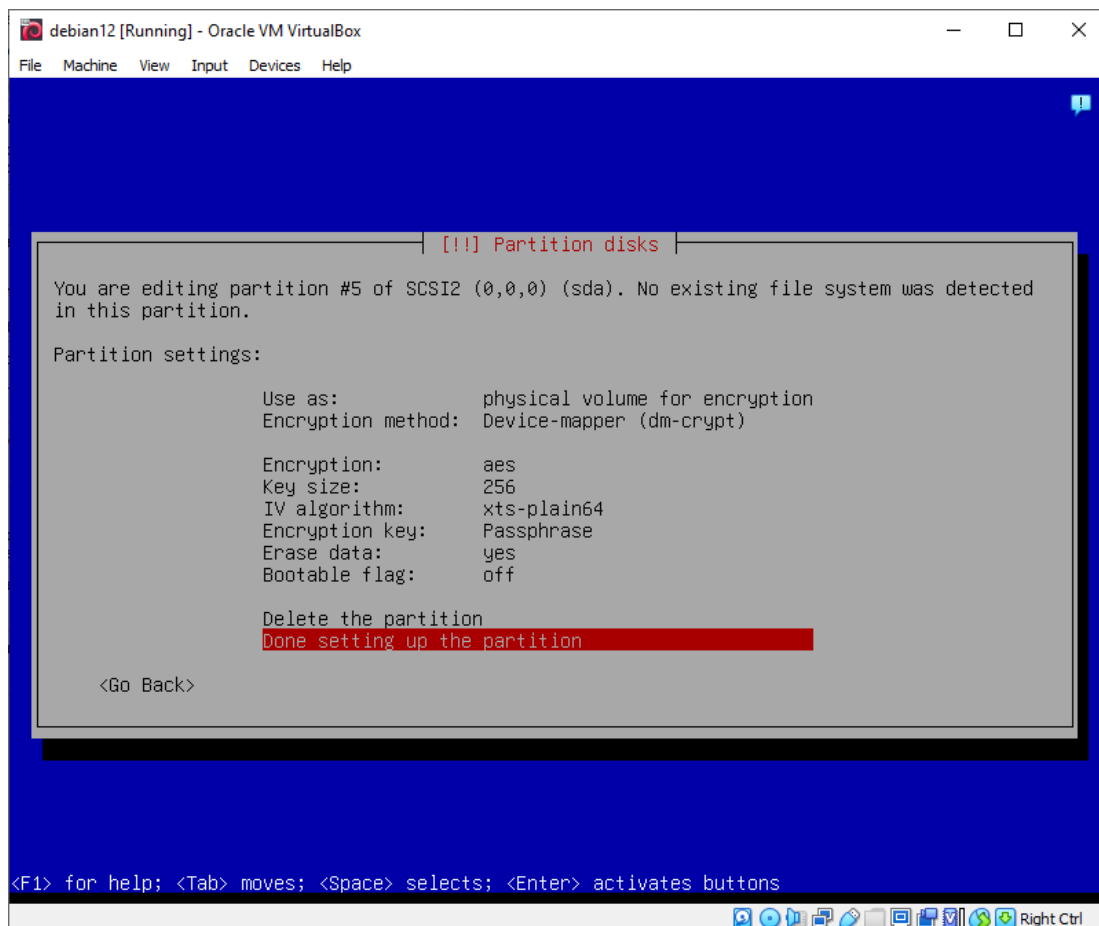
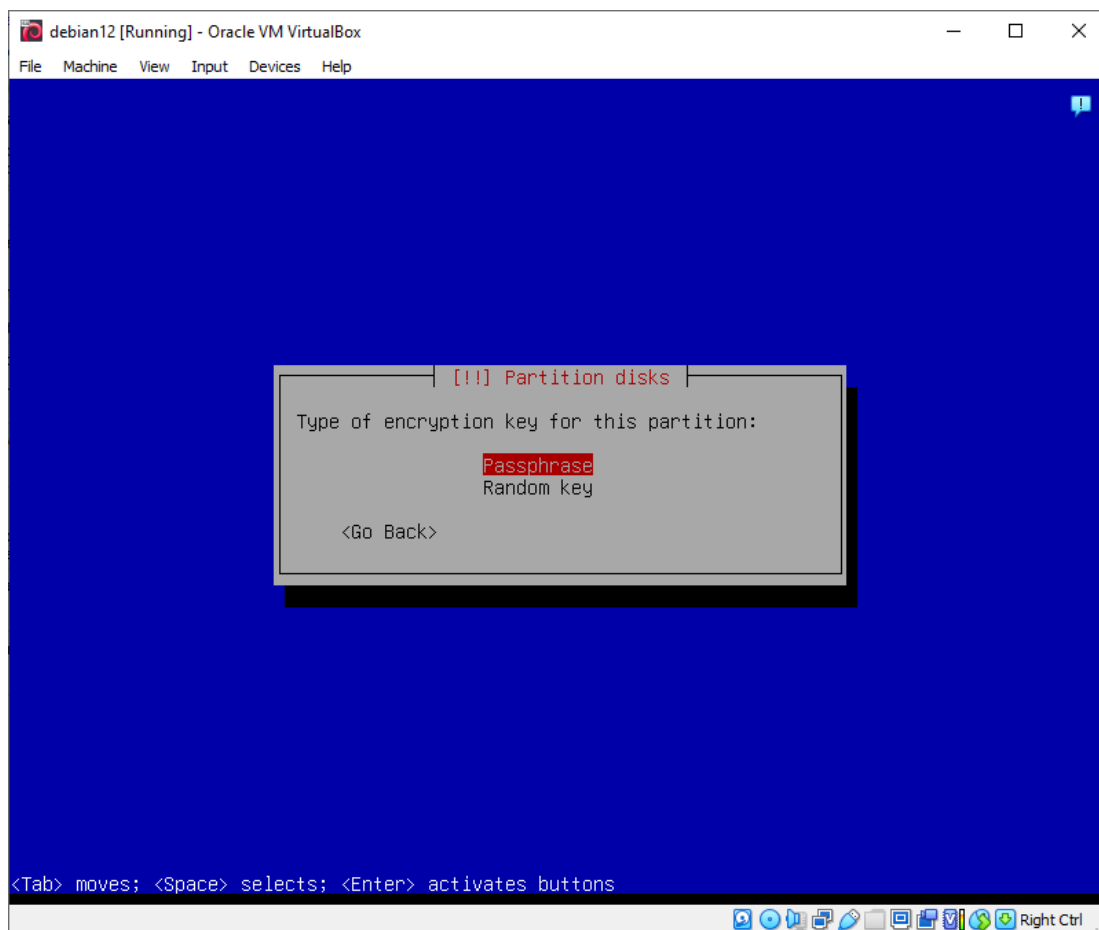
Select Done and press enter



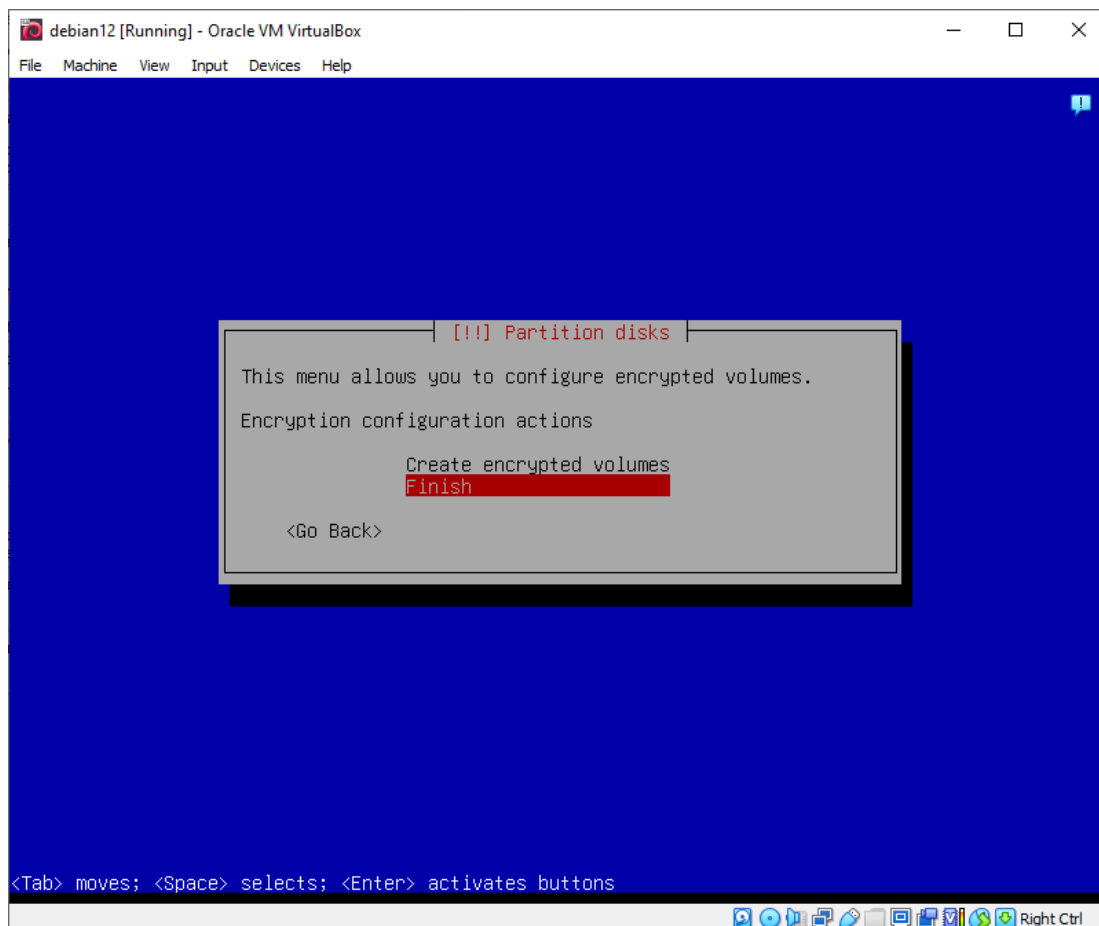
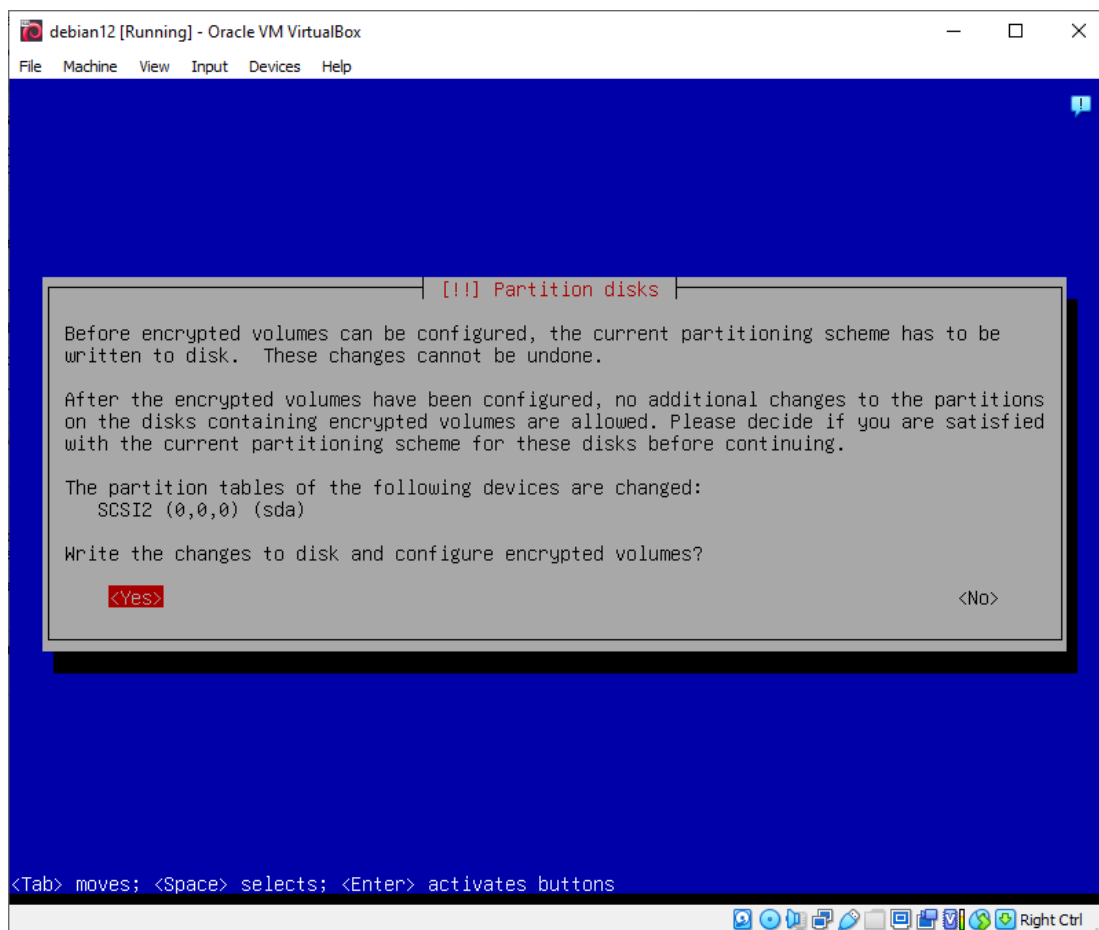


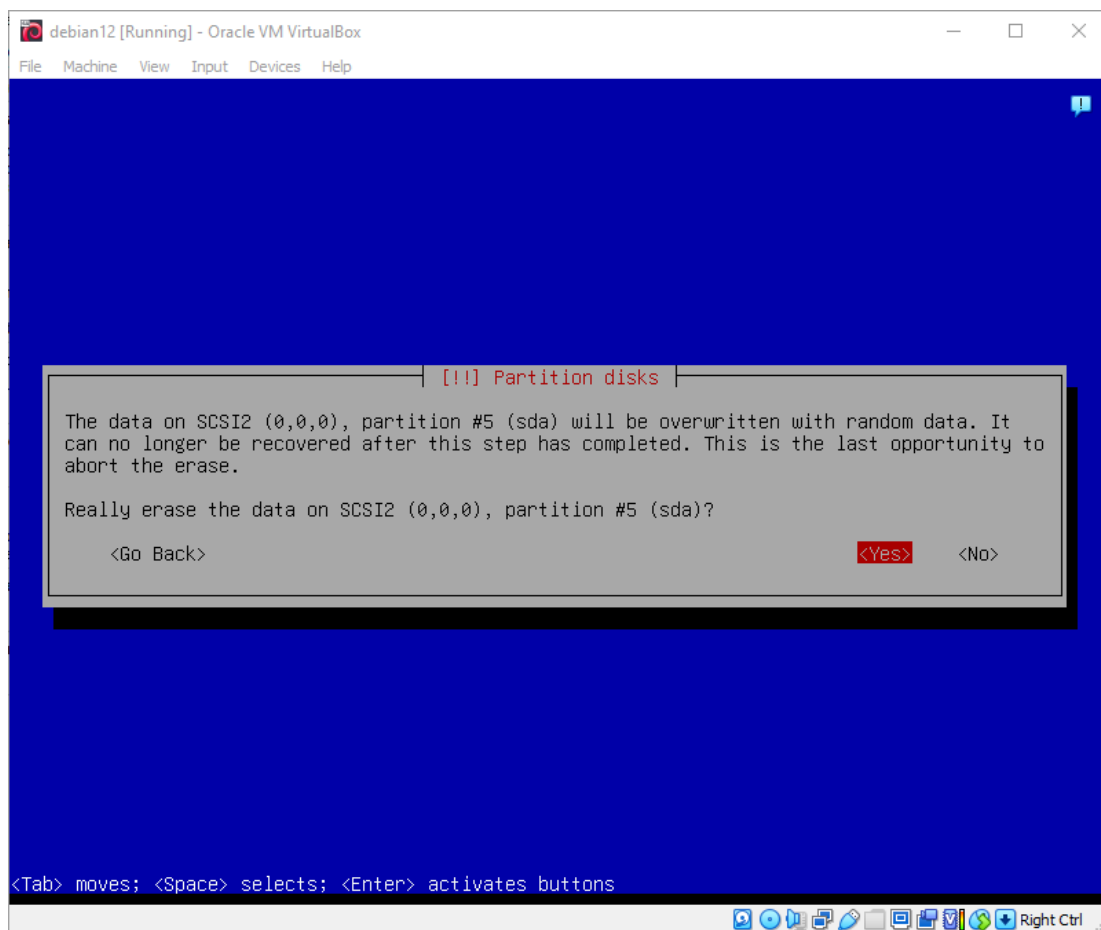
Select the free space



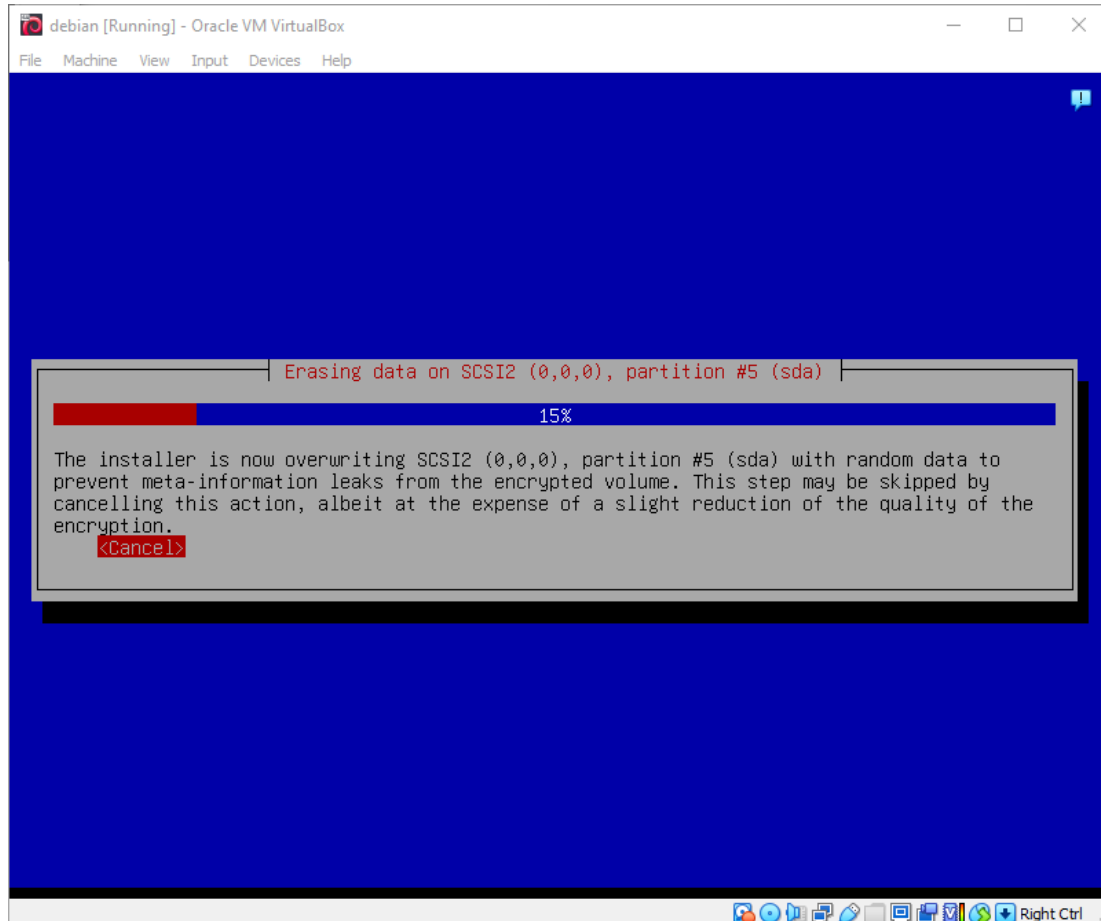






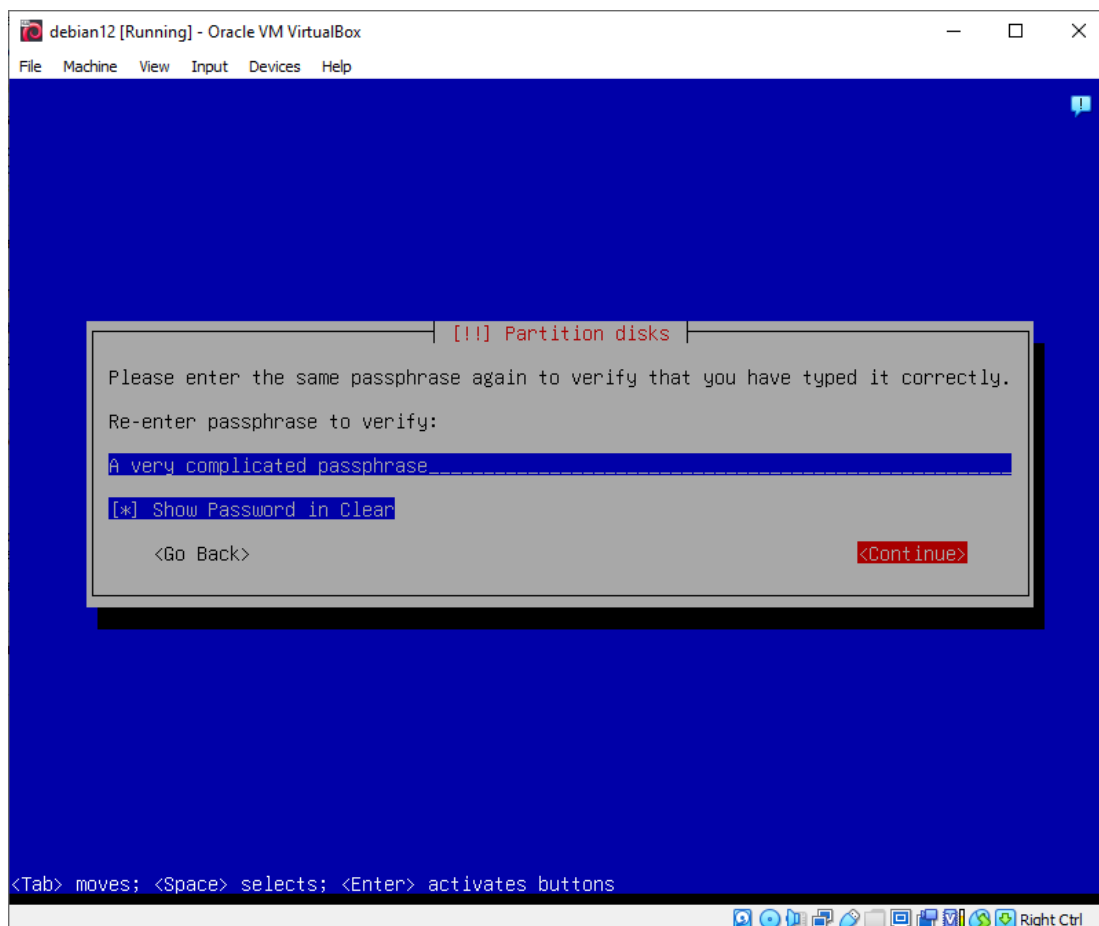
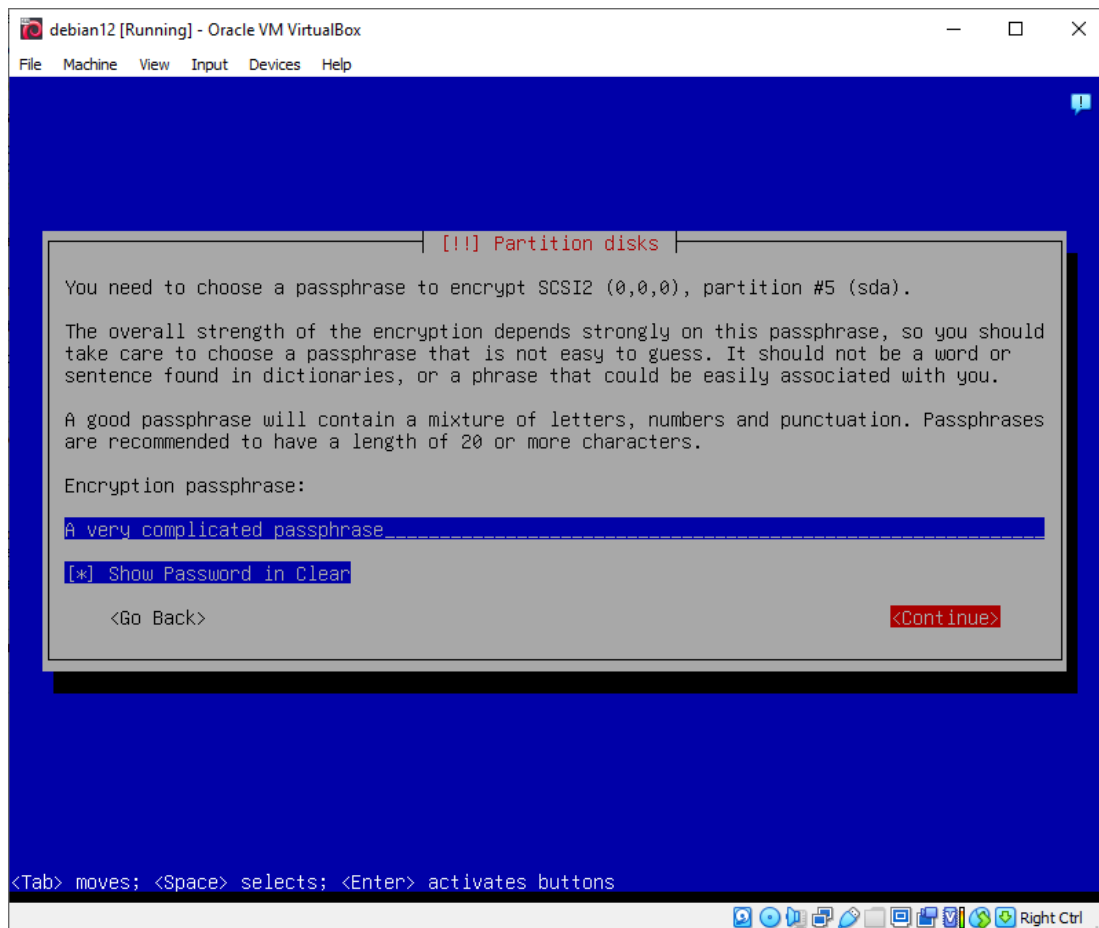


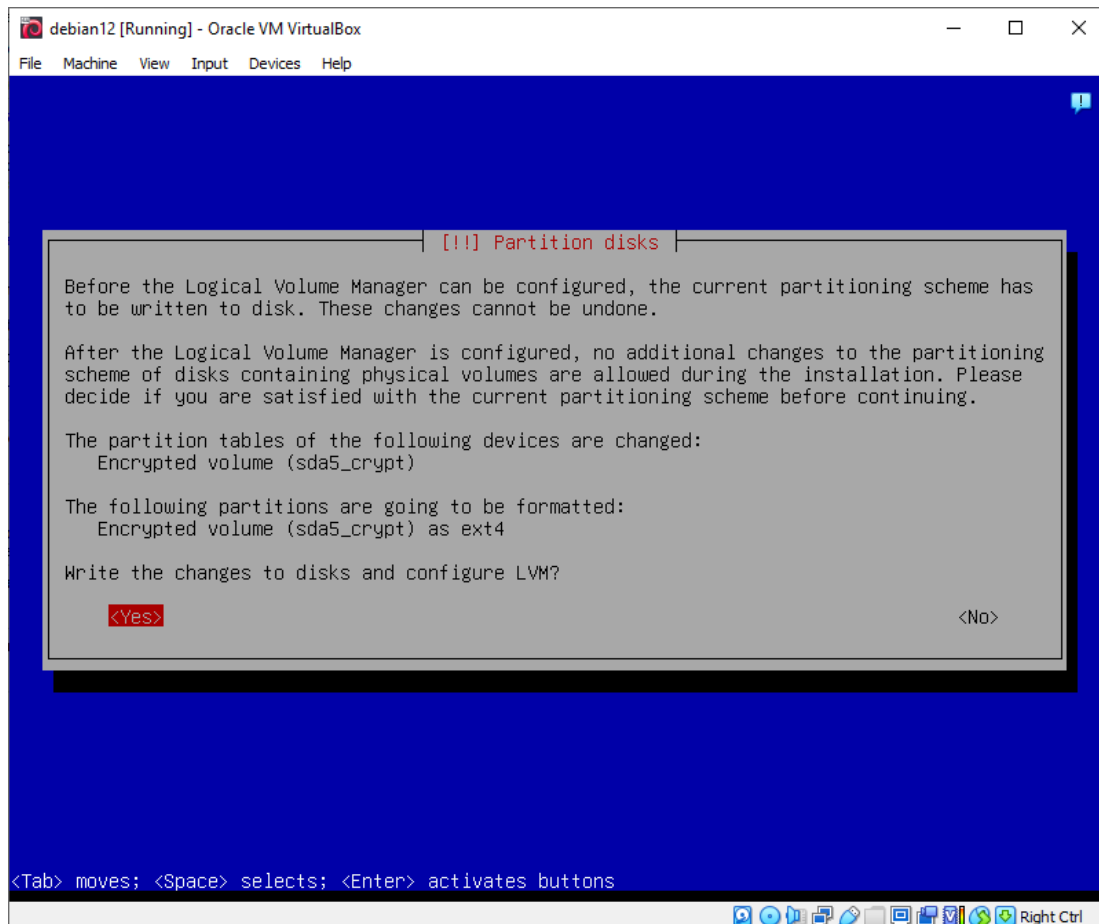
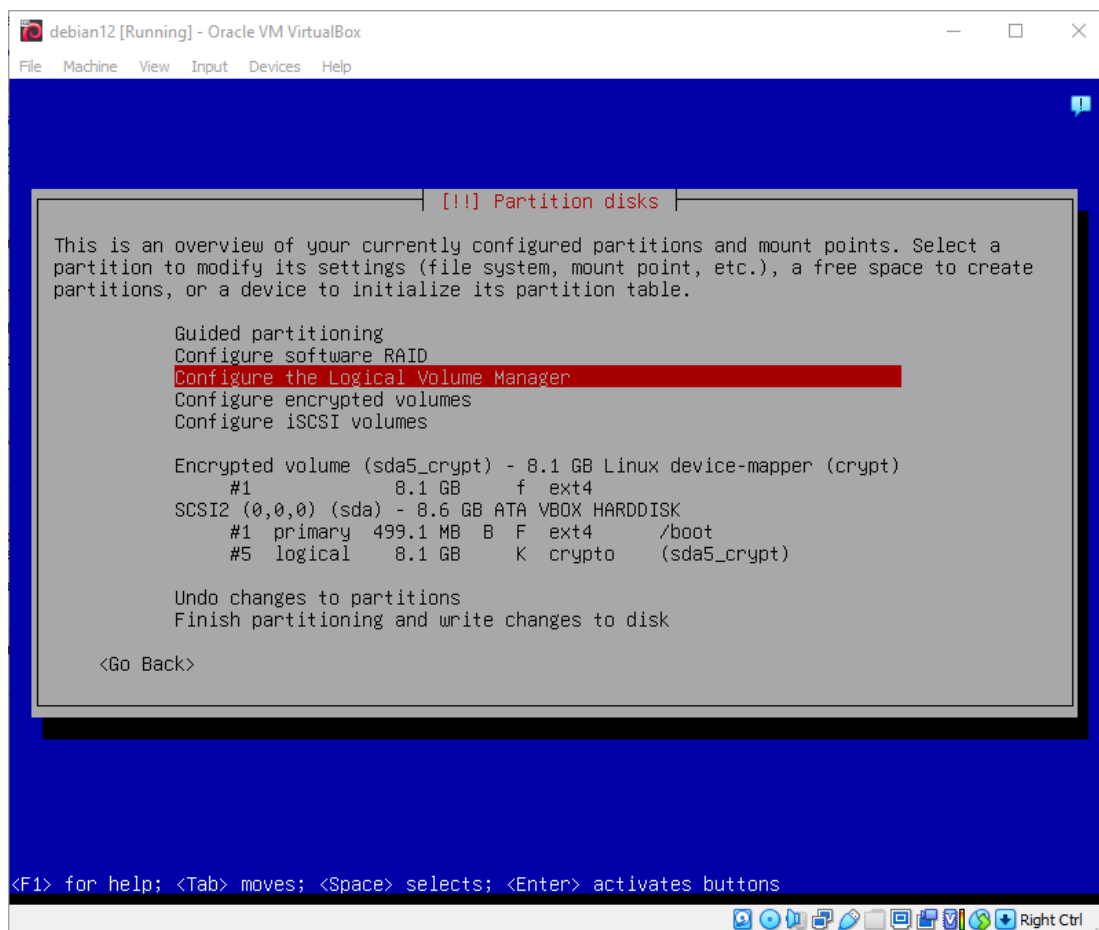
Virtual disk is erased first

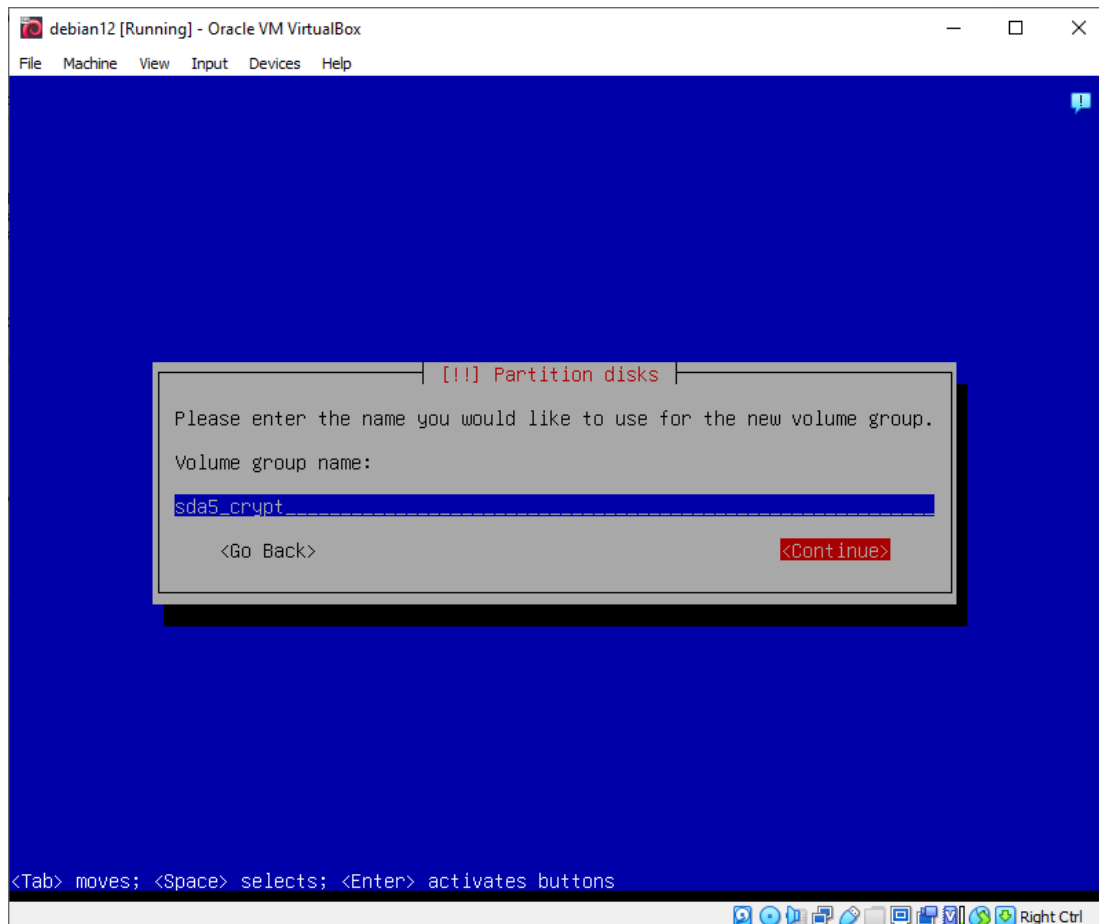
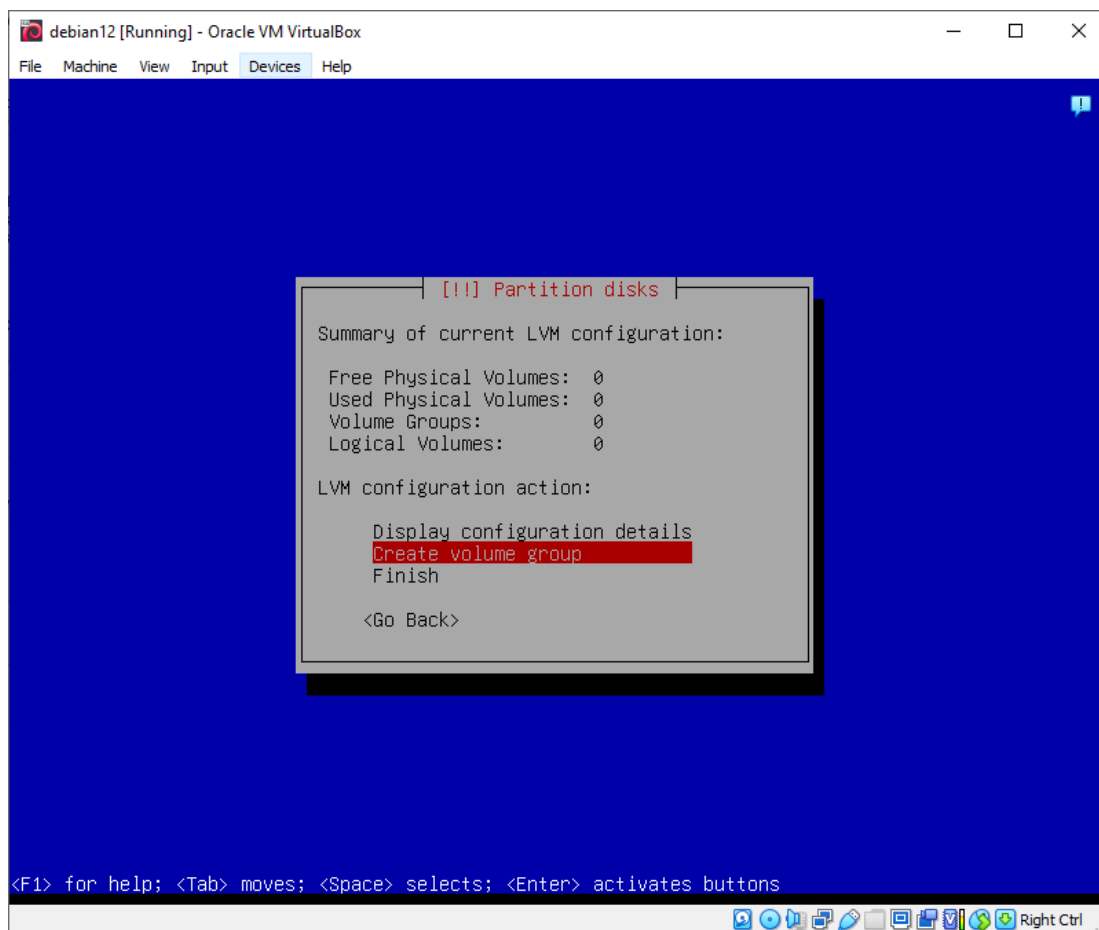


Specify a passphrase to be used for encrypting the volume - this is needed at boot time to decrypt the volume!

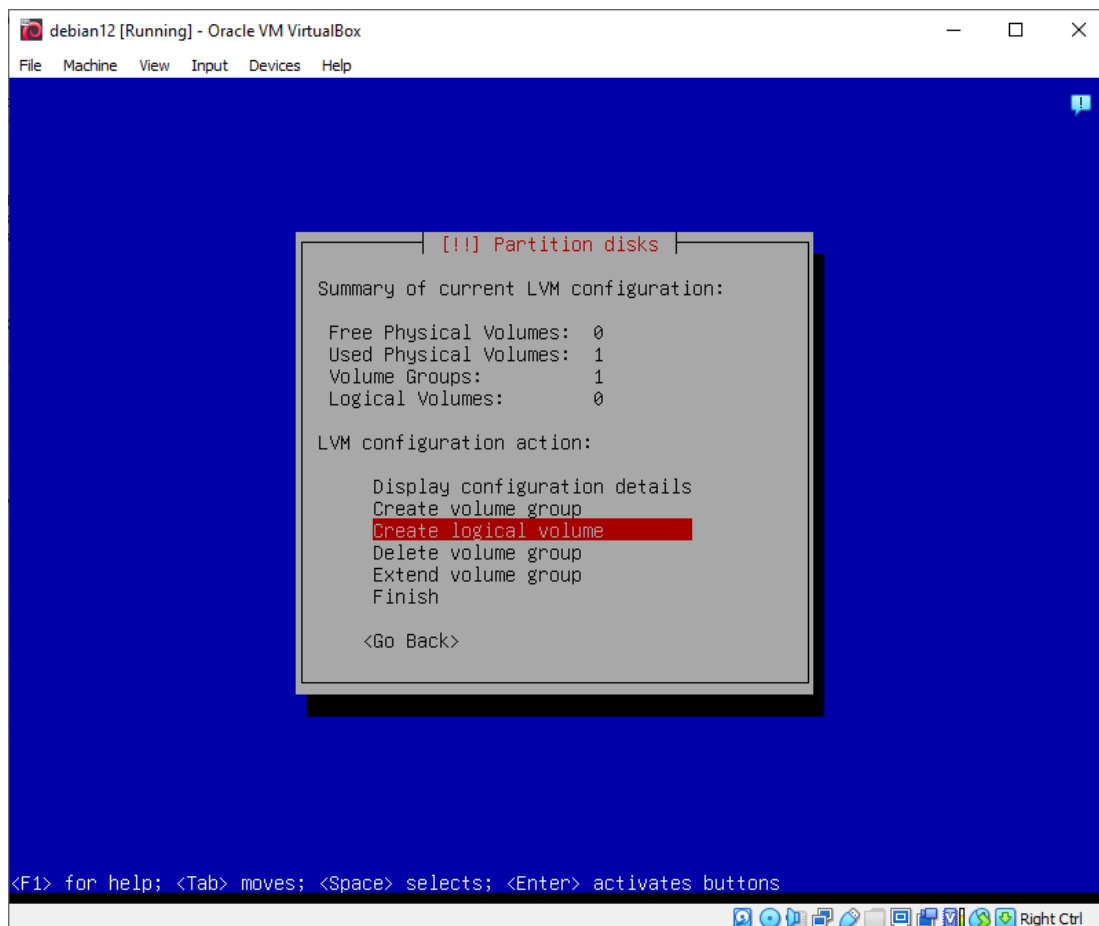
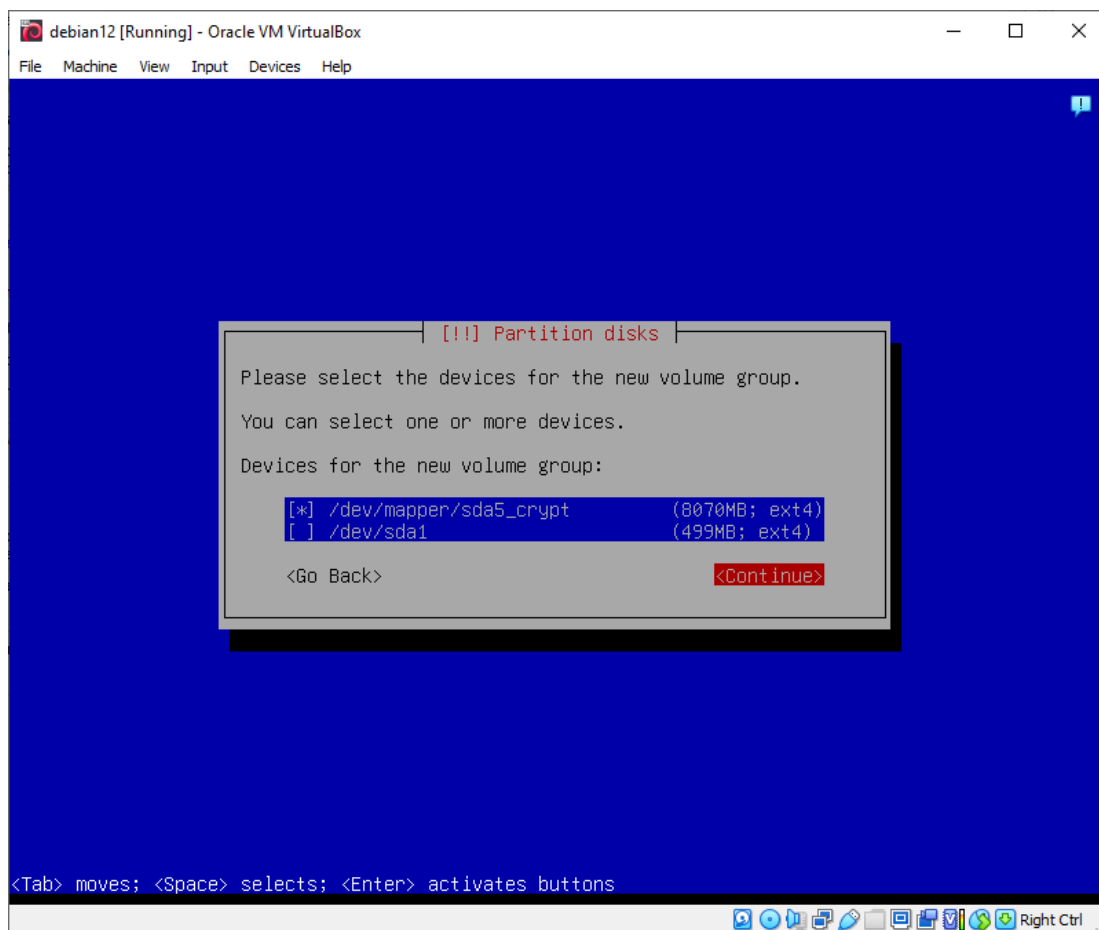
A very complicated passphrase

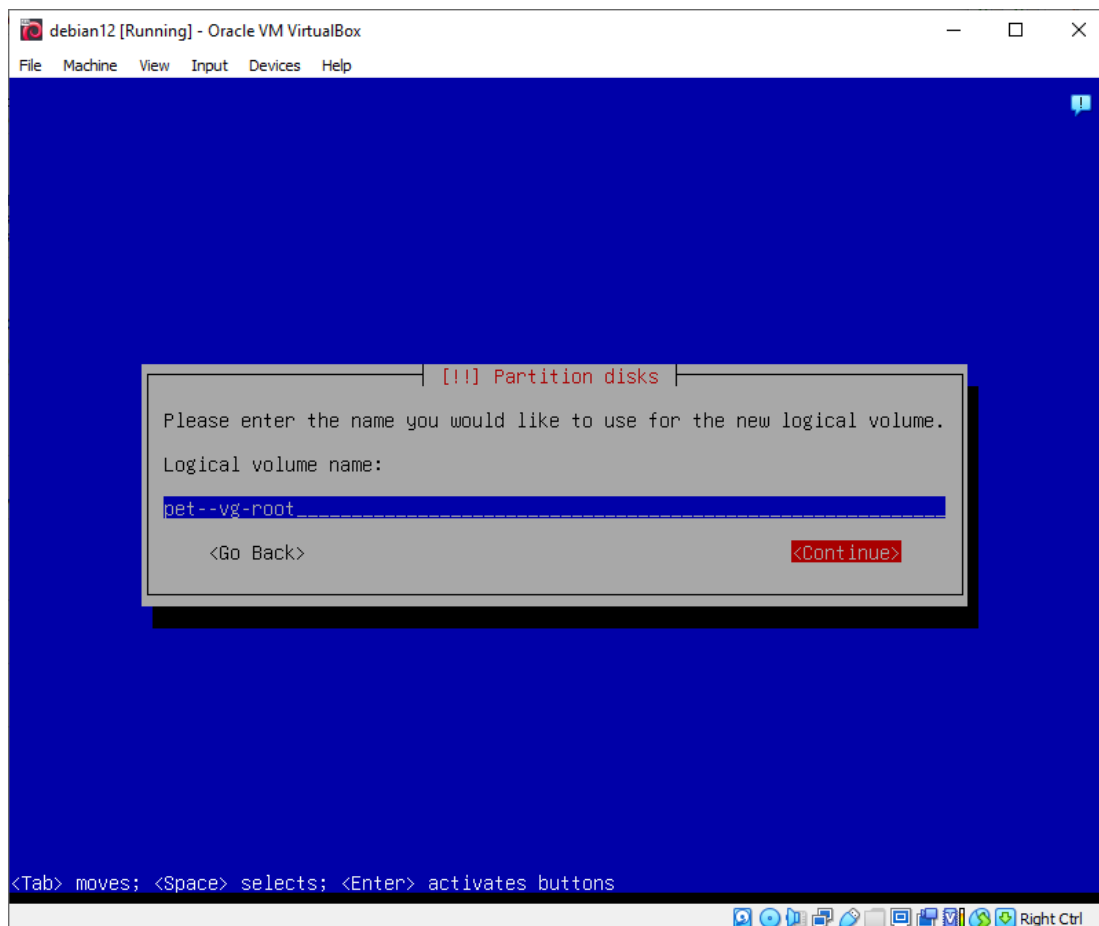
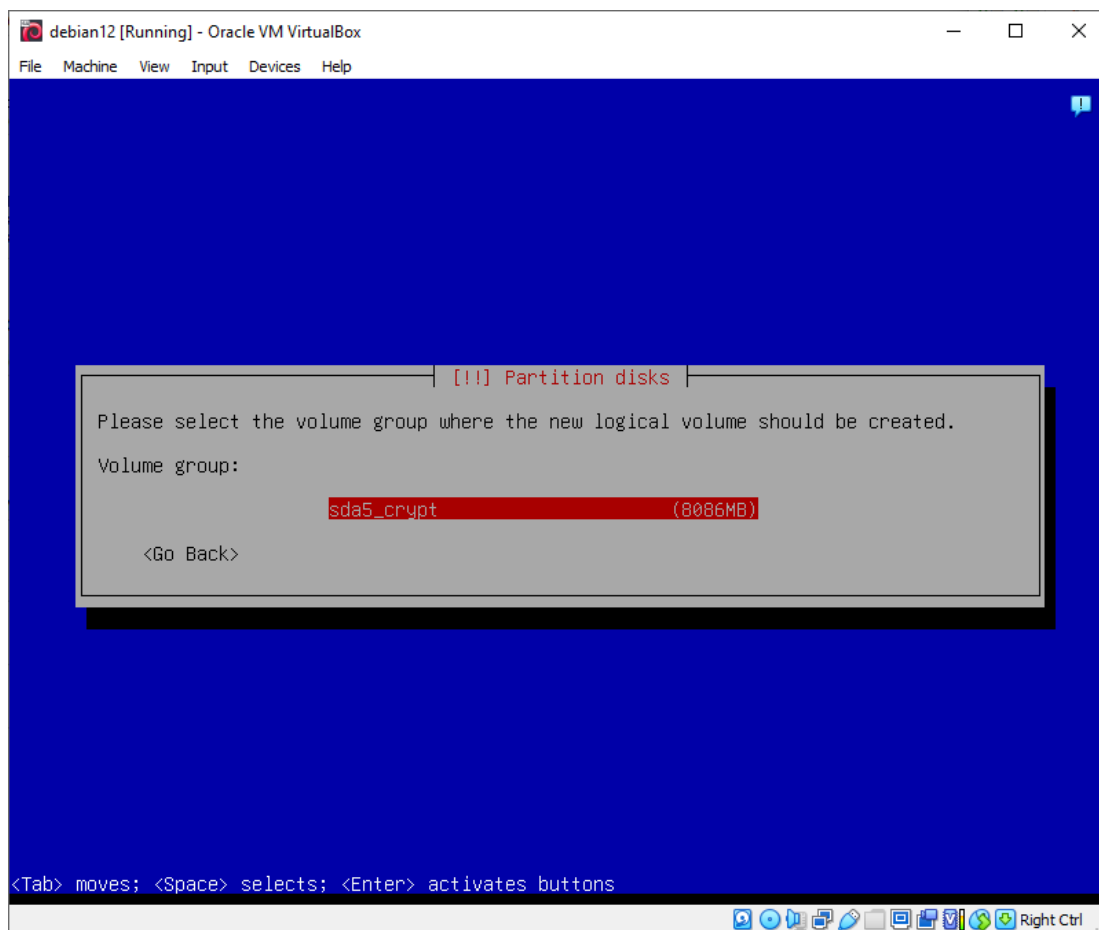


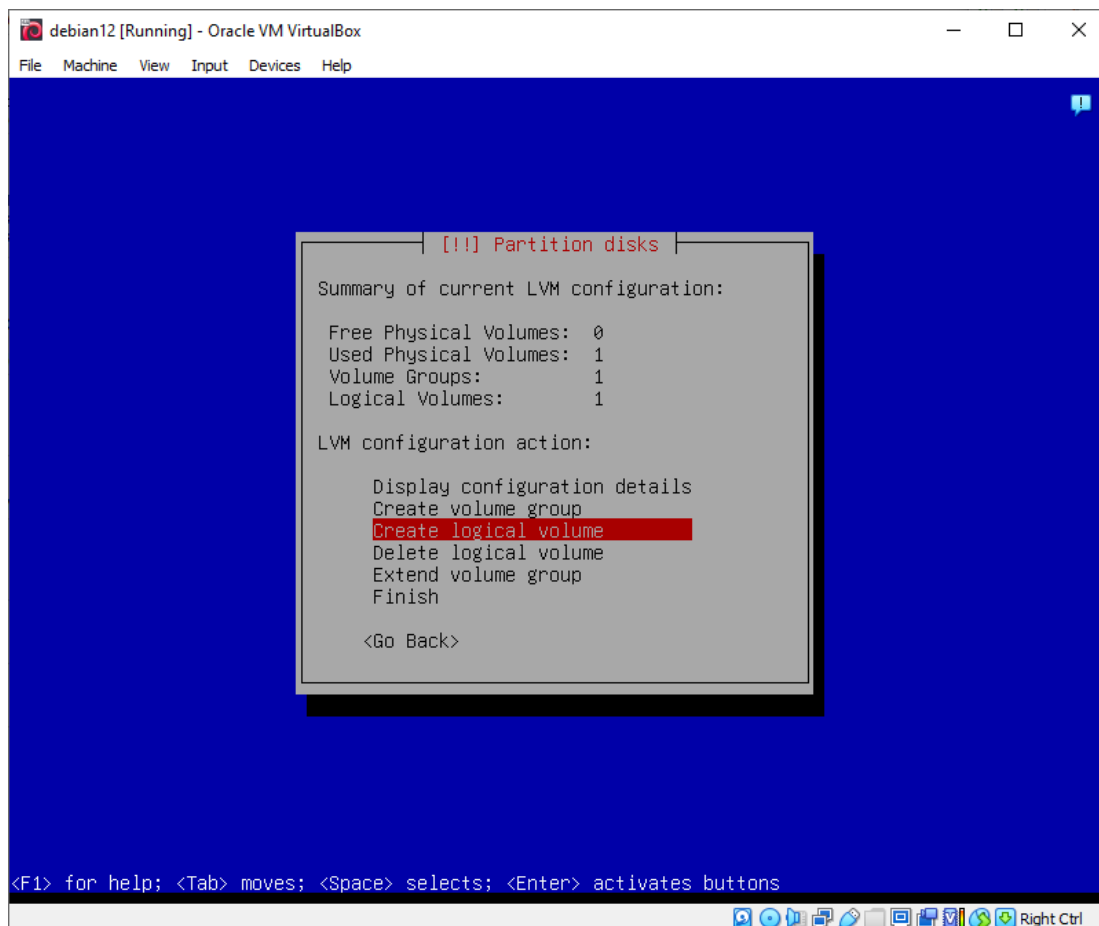
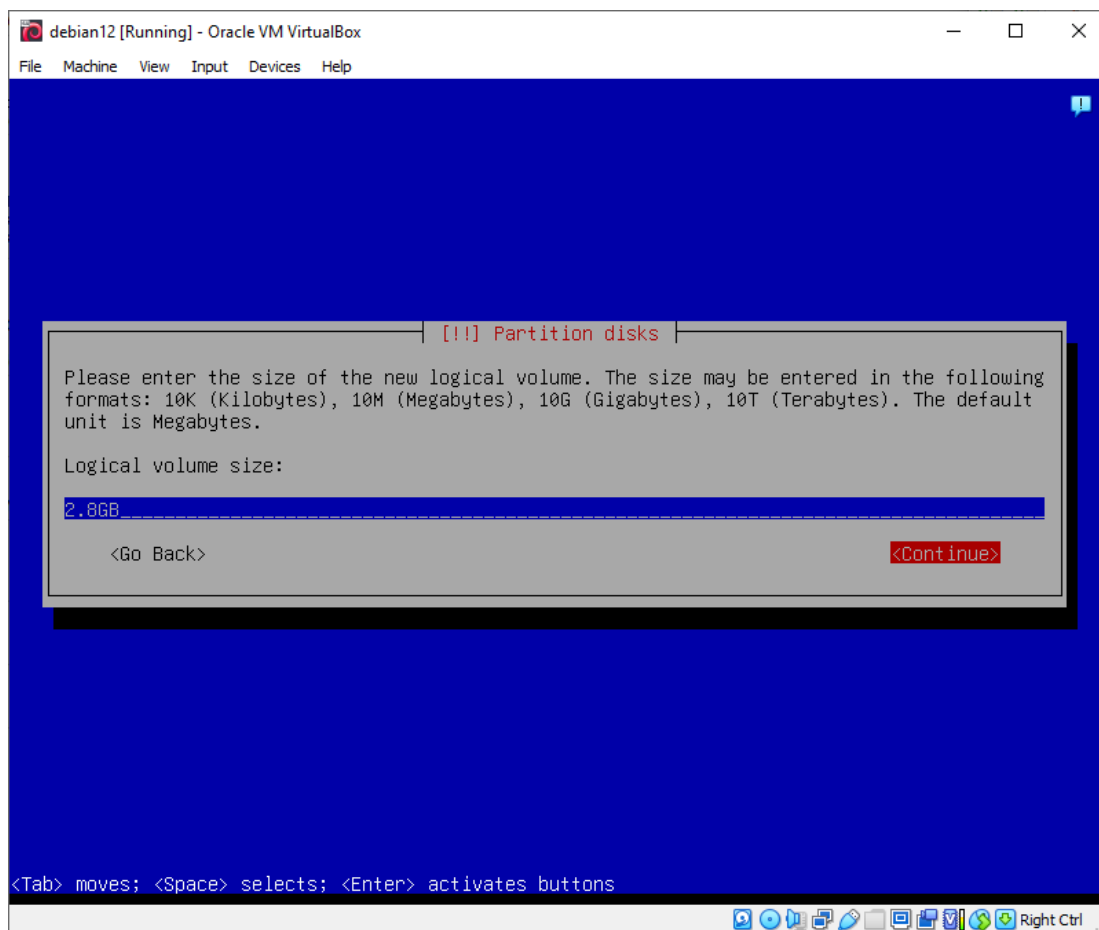




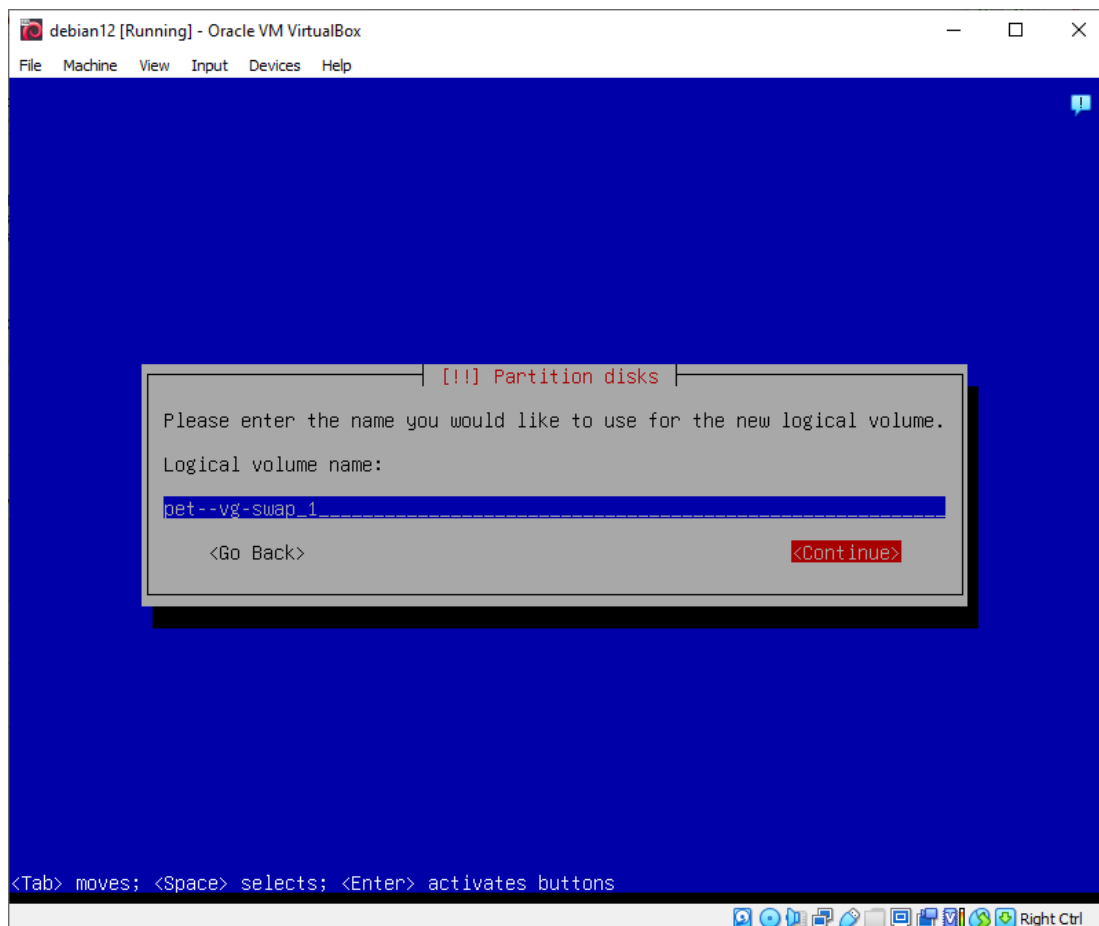
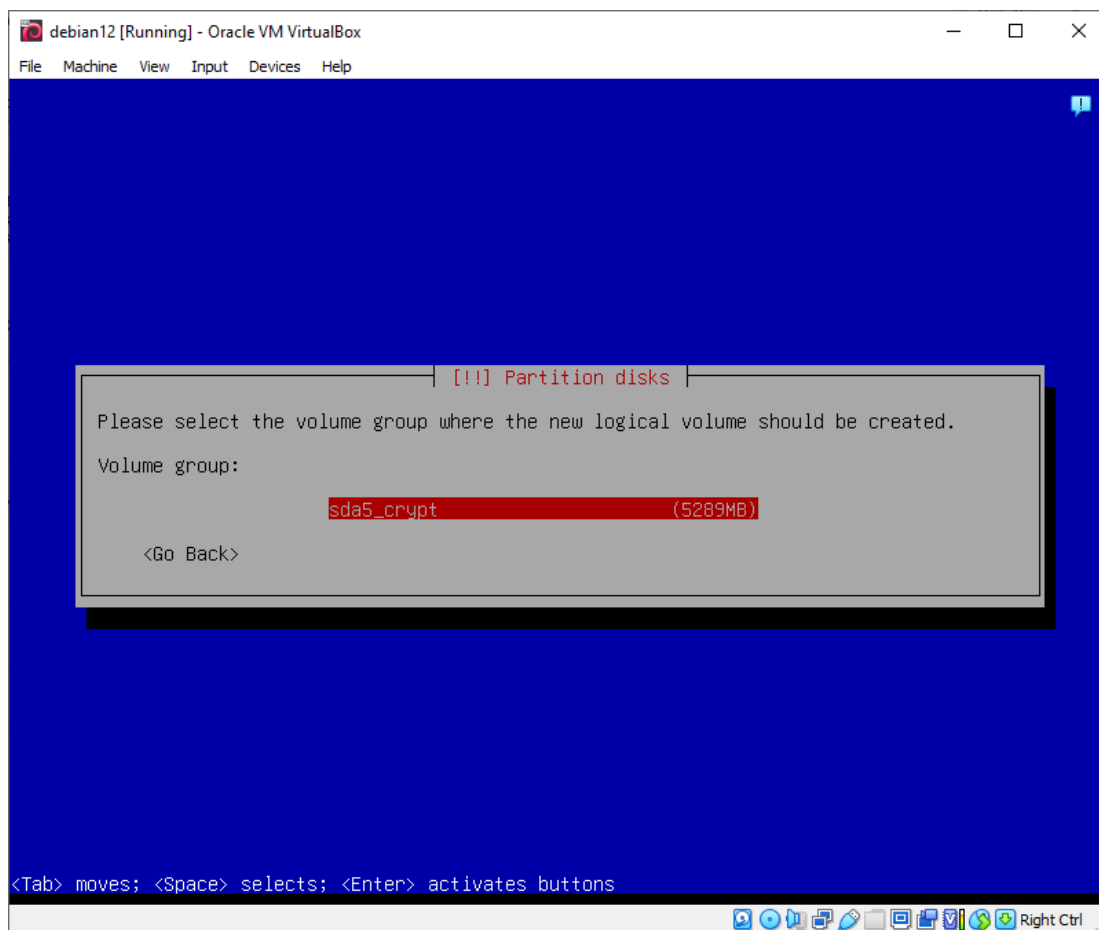
Select /dev/mapper/sda5\_crypt

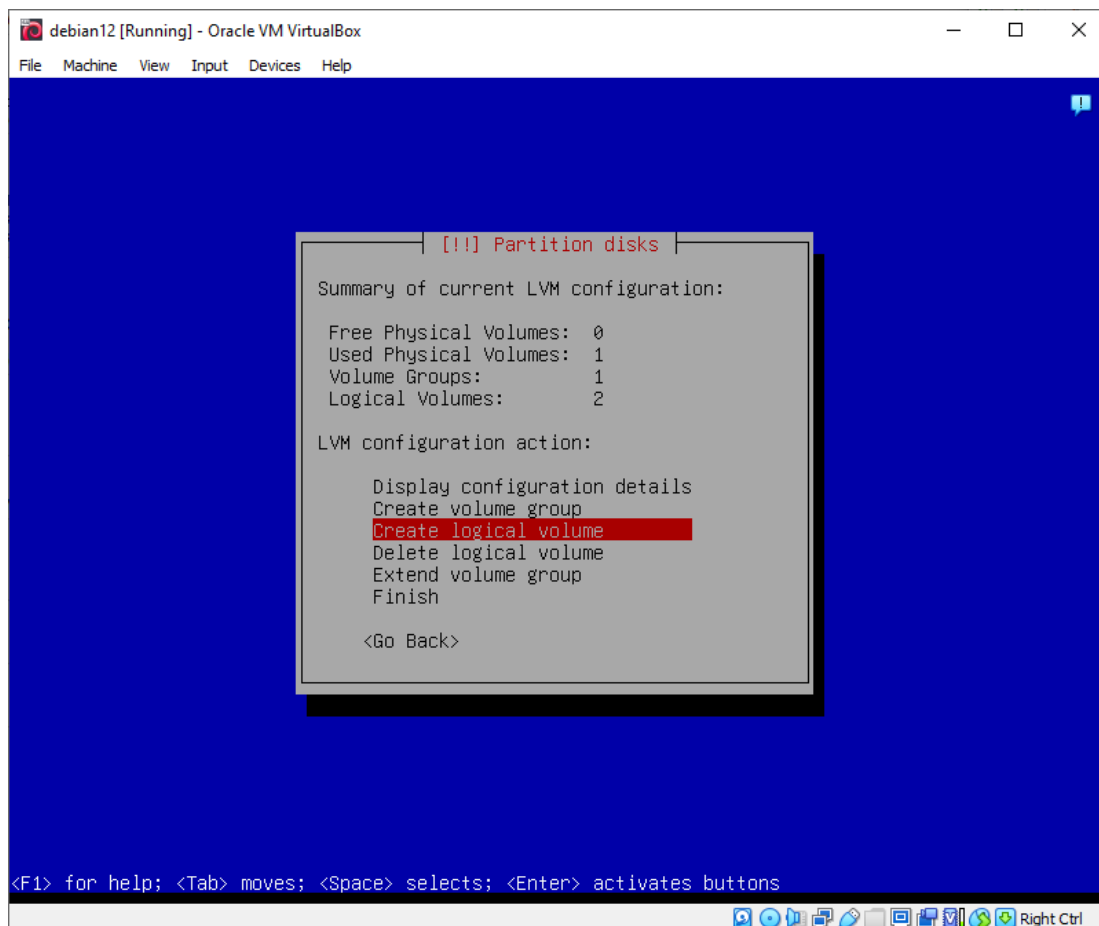
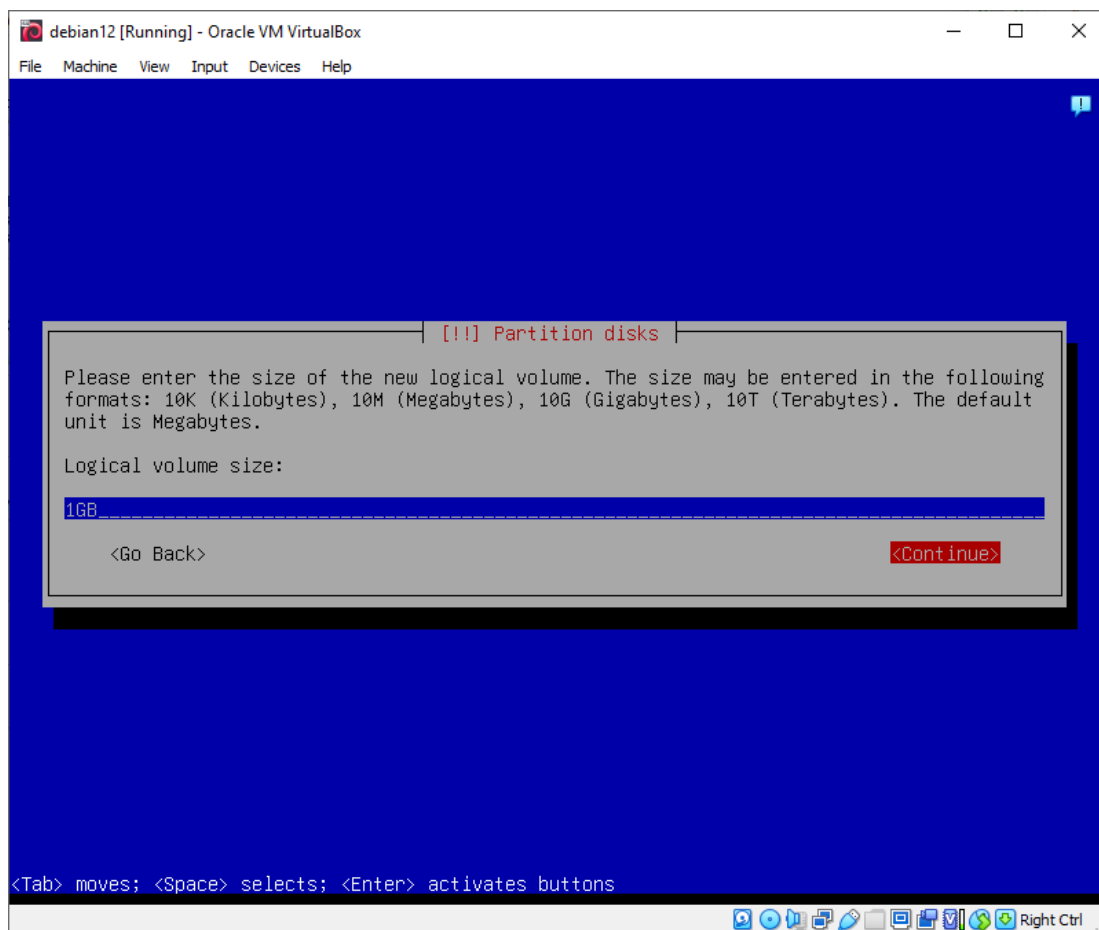


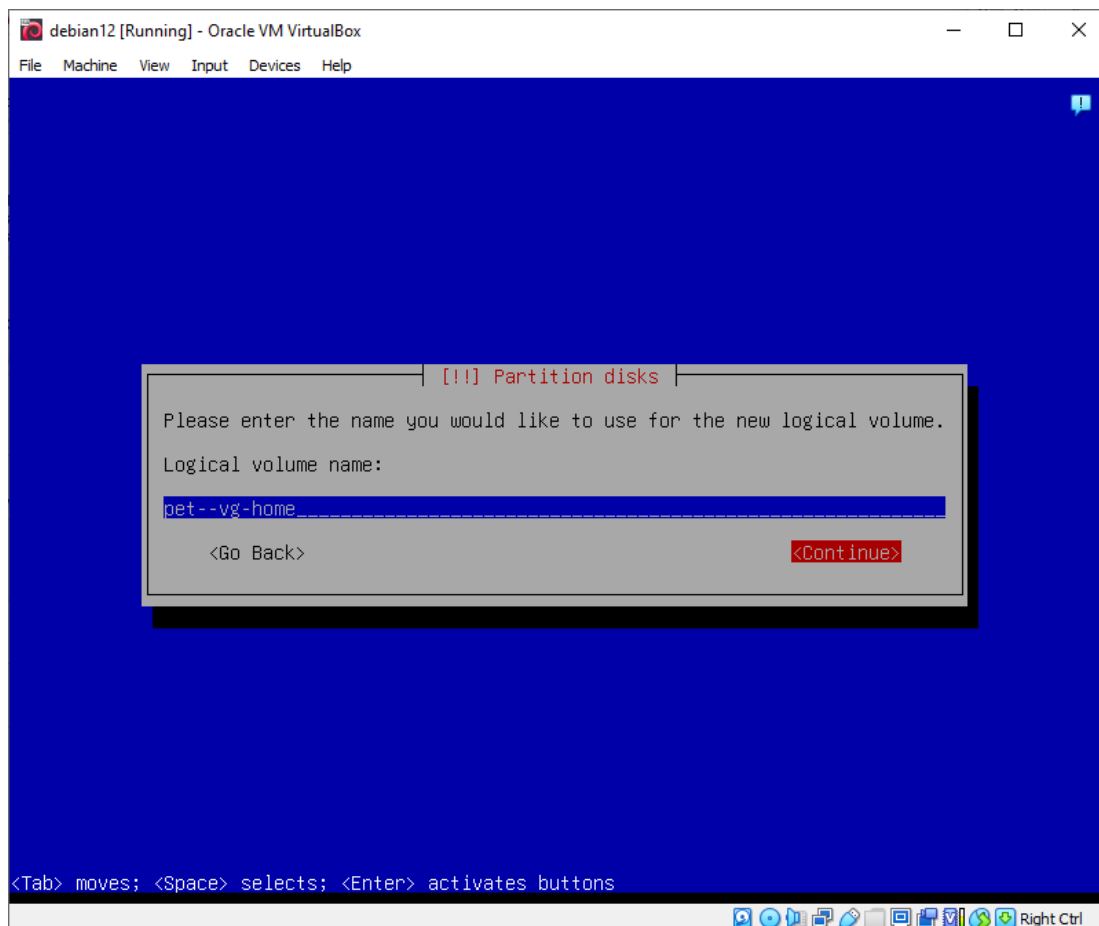
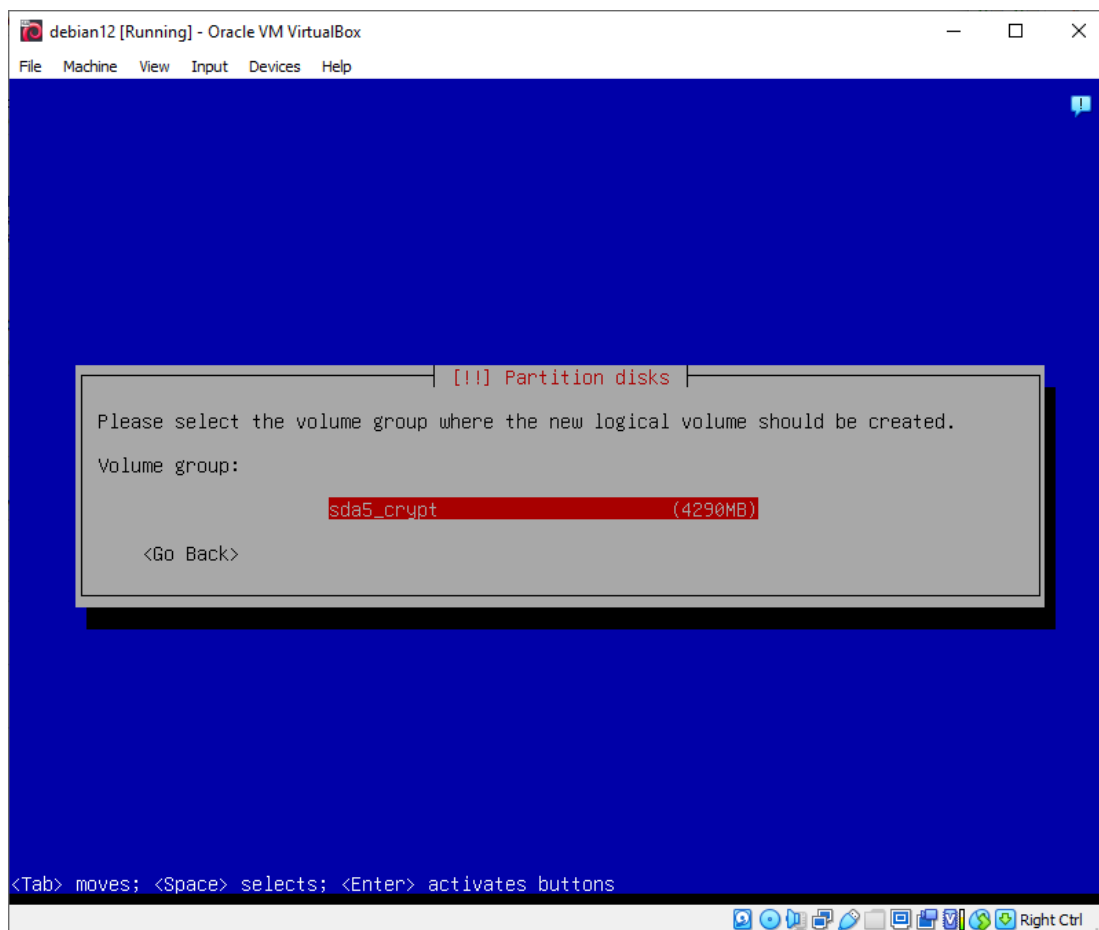


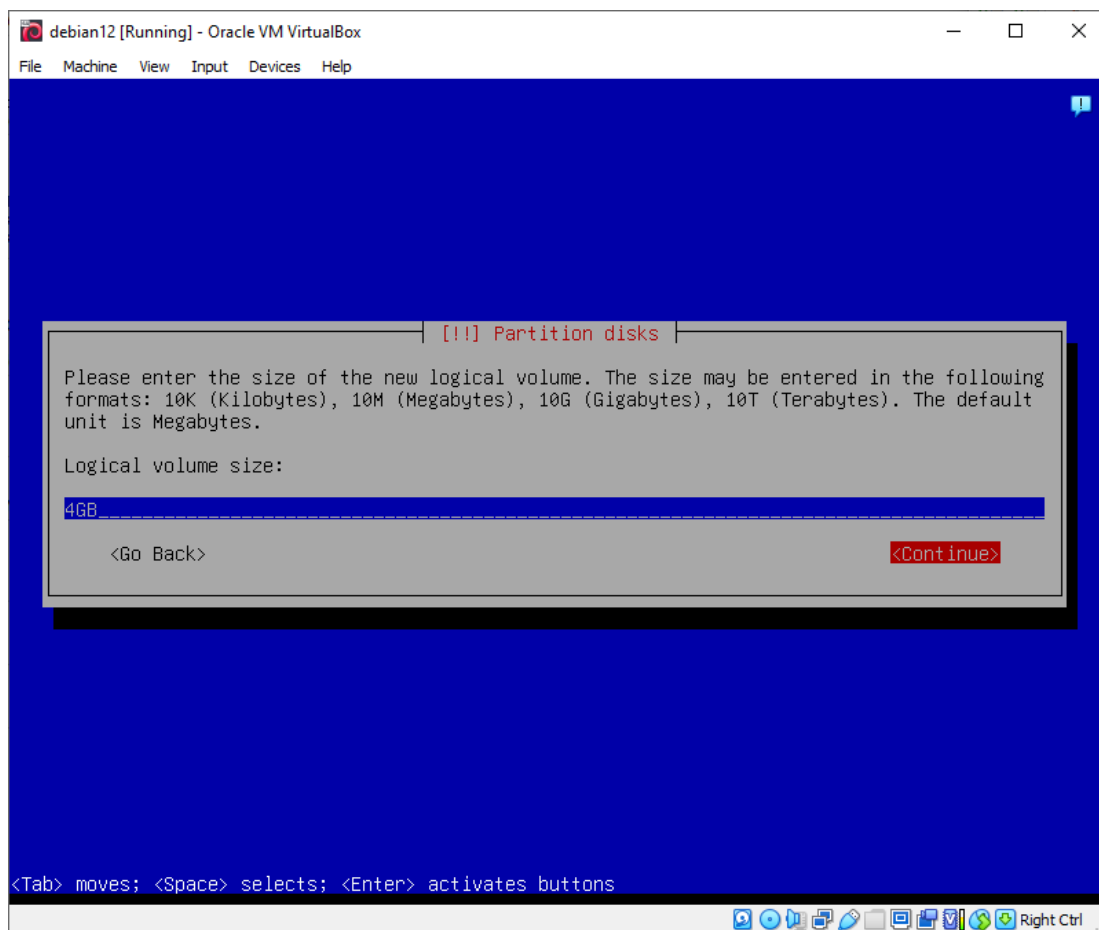




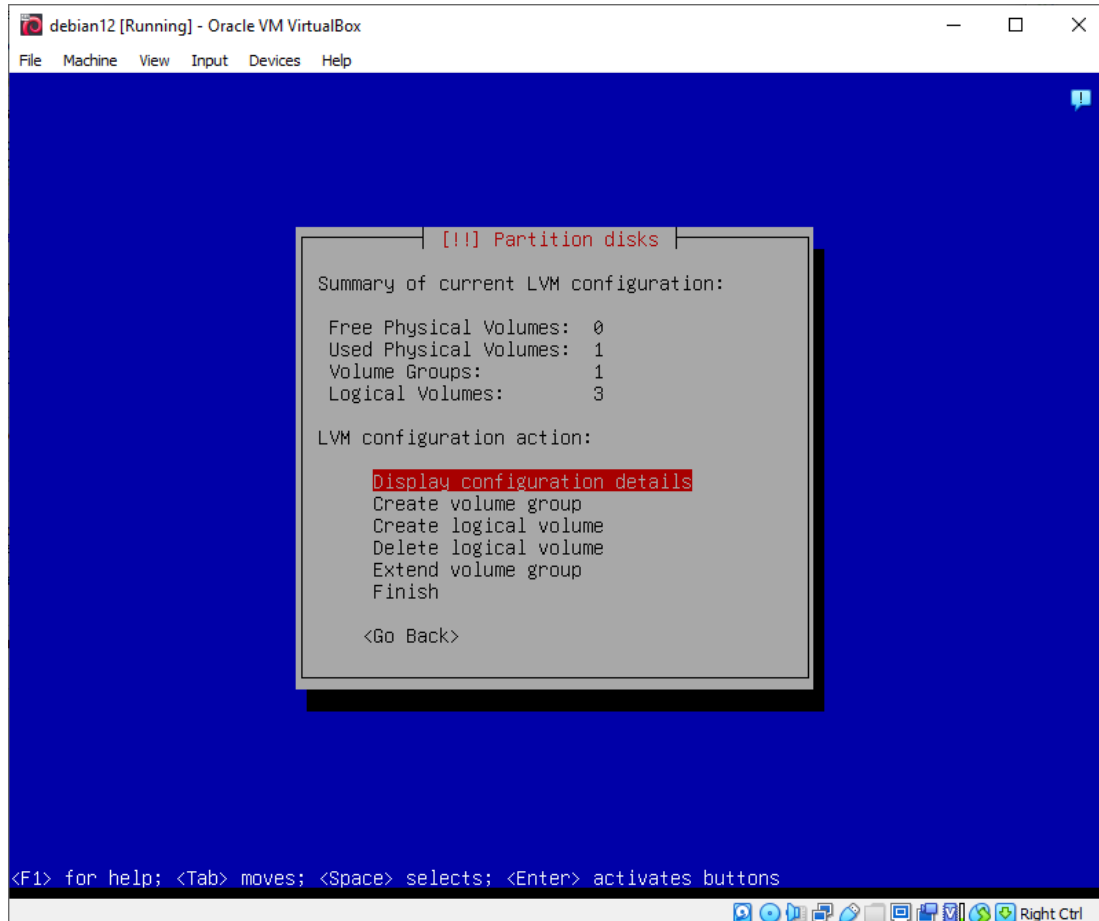


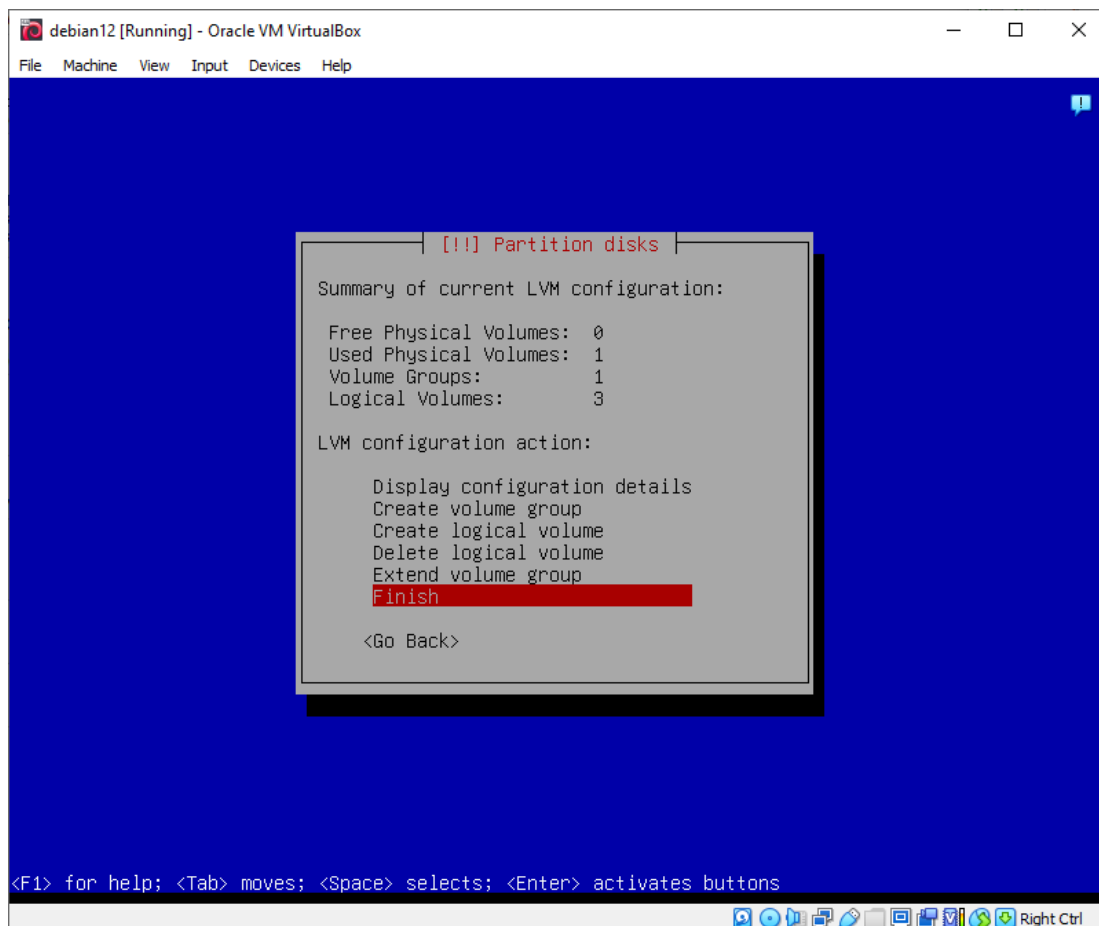
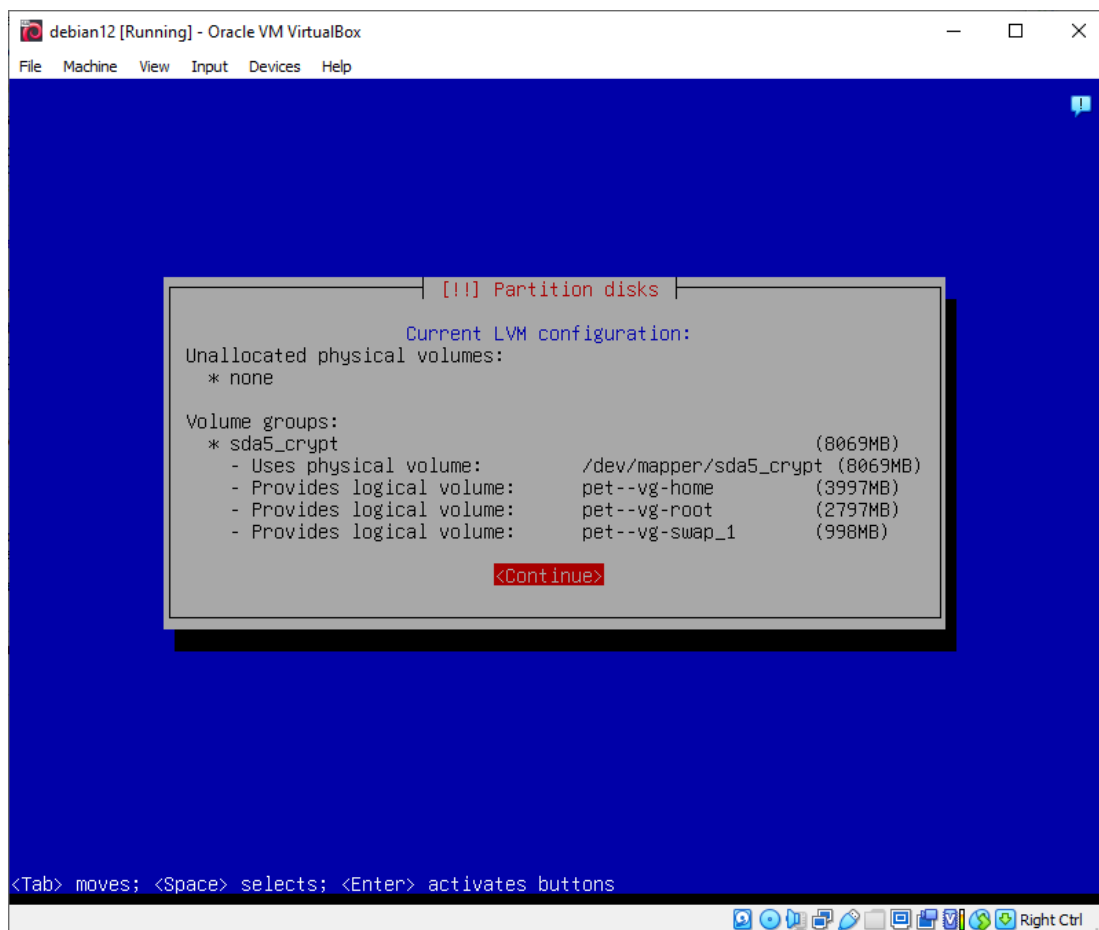


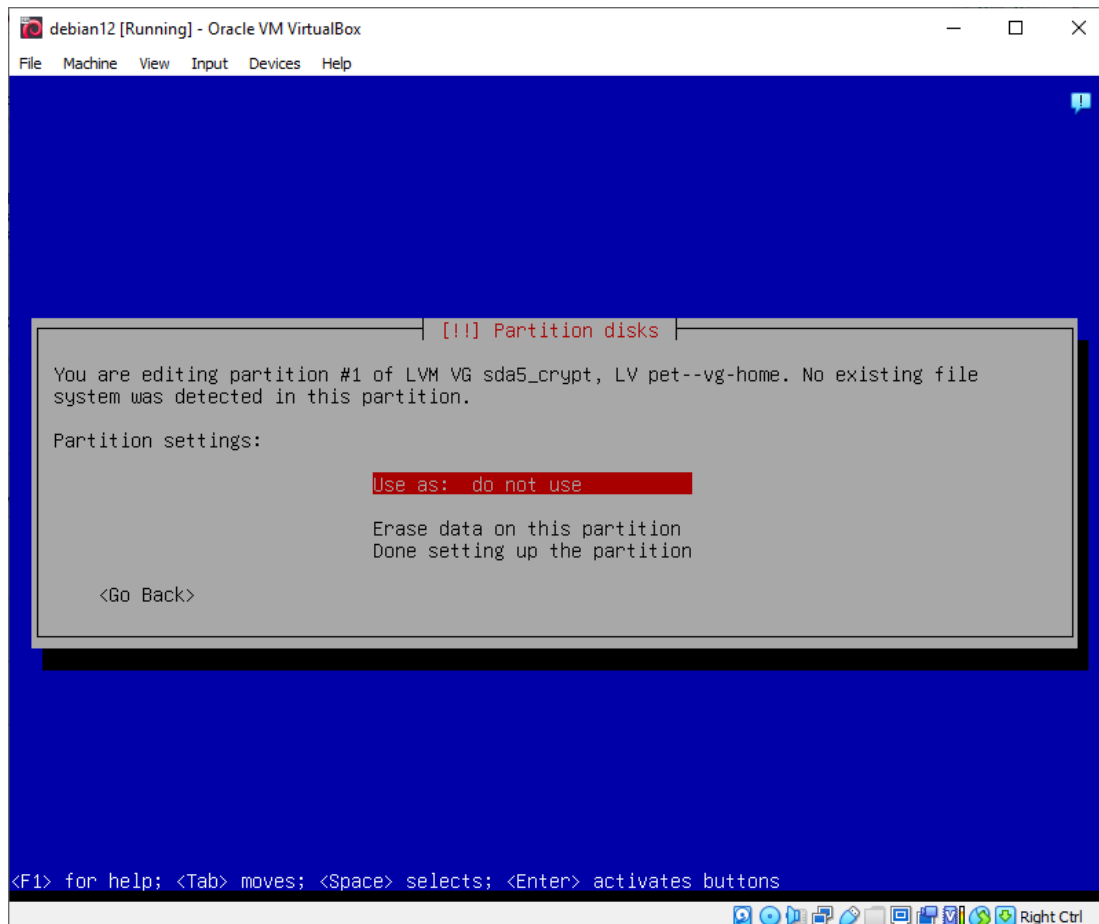
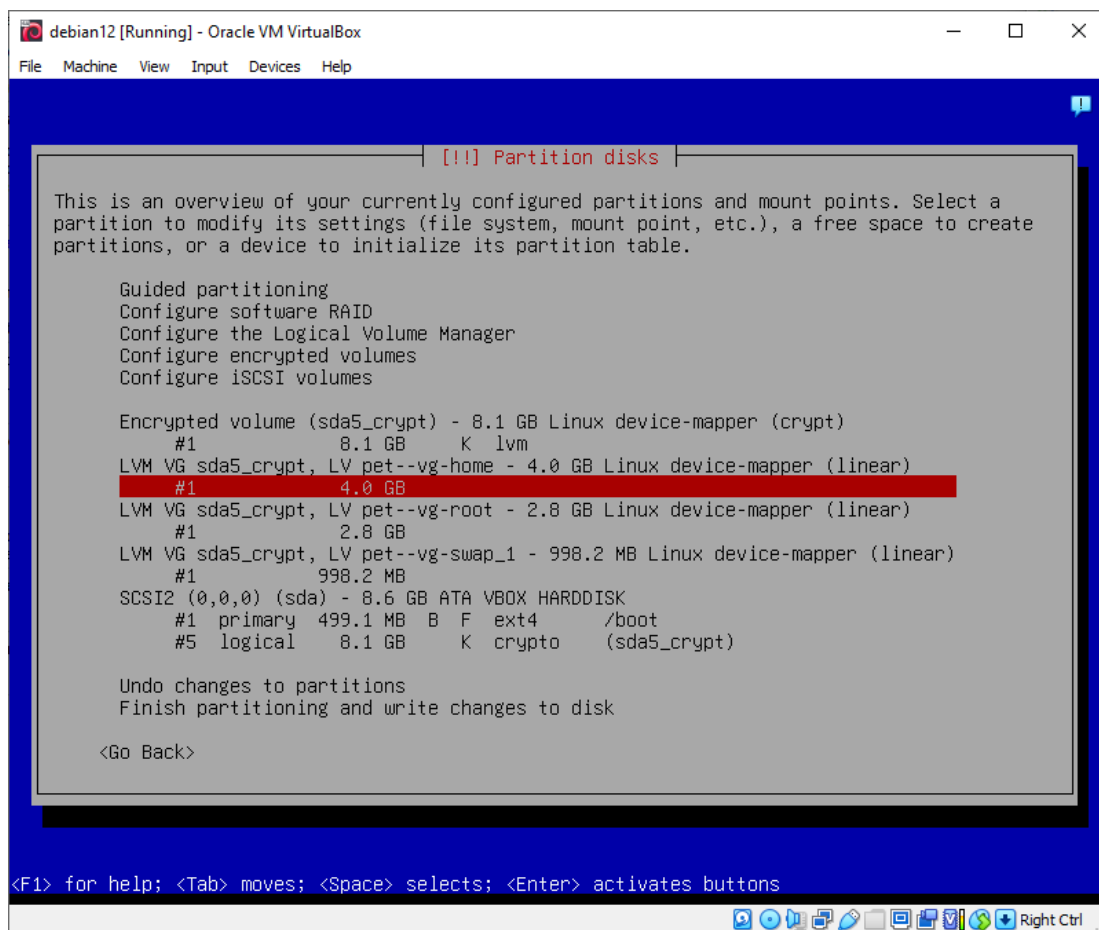


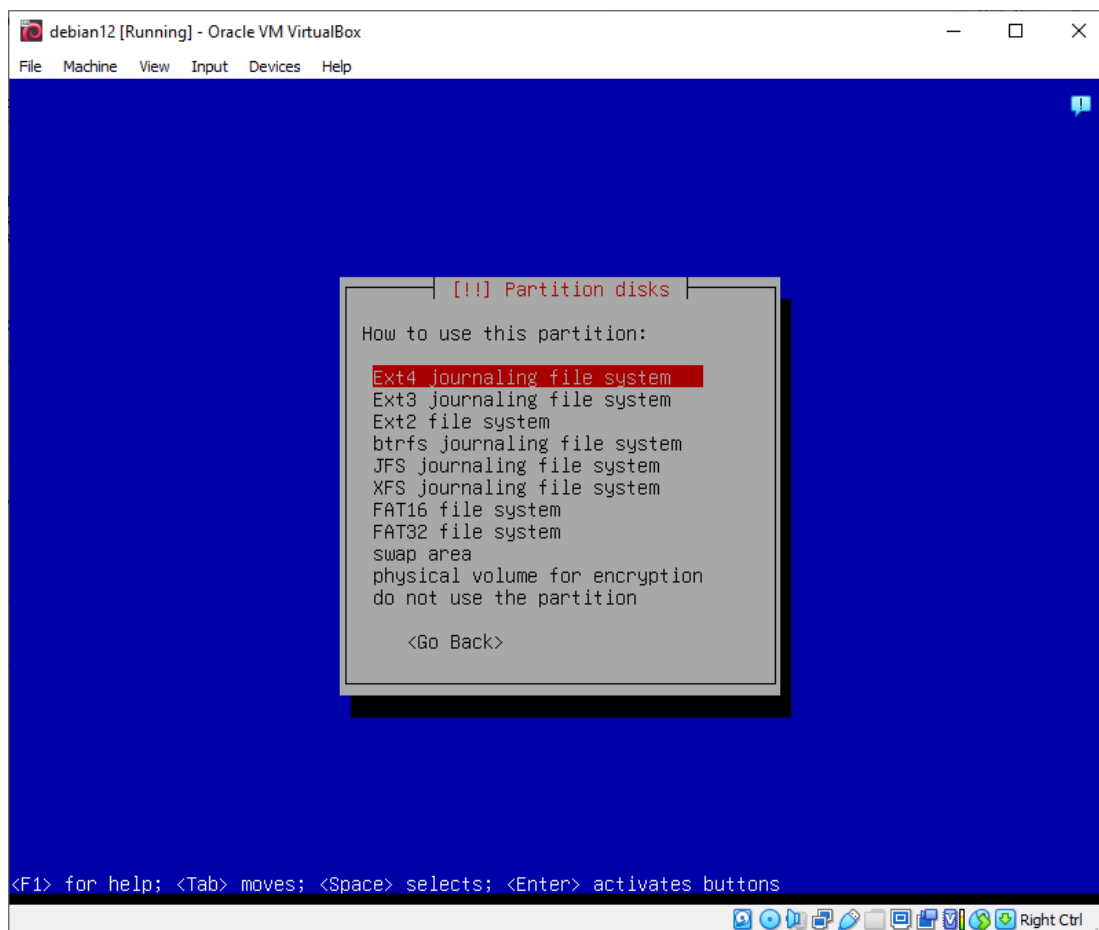


Display configuration values to verify configuration

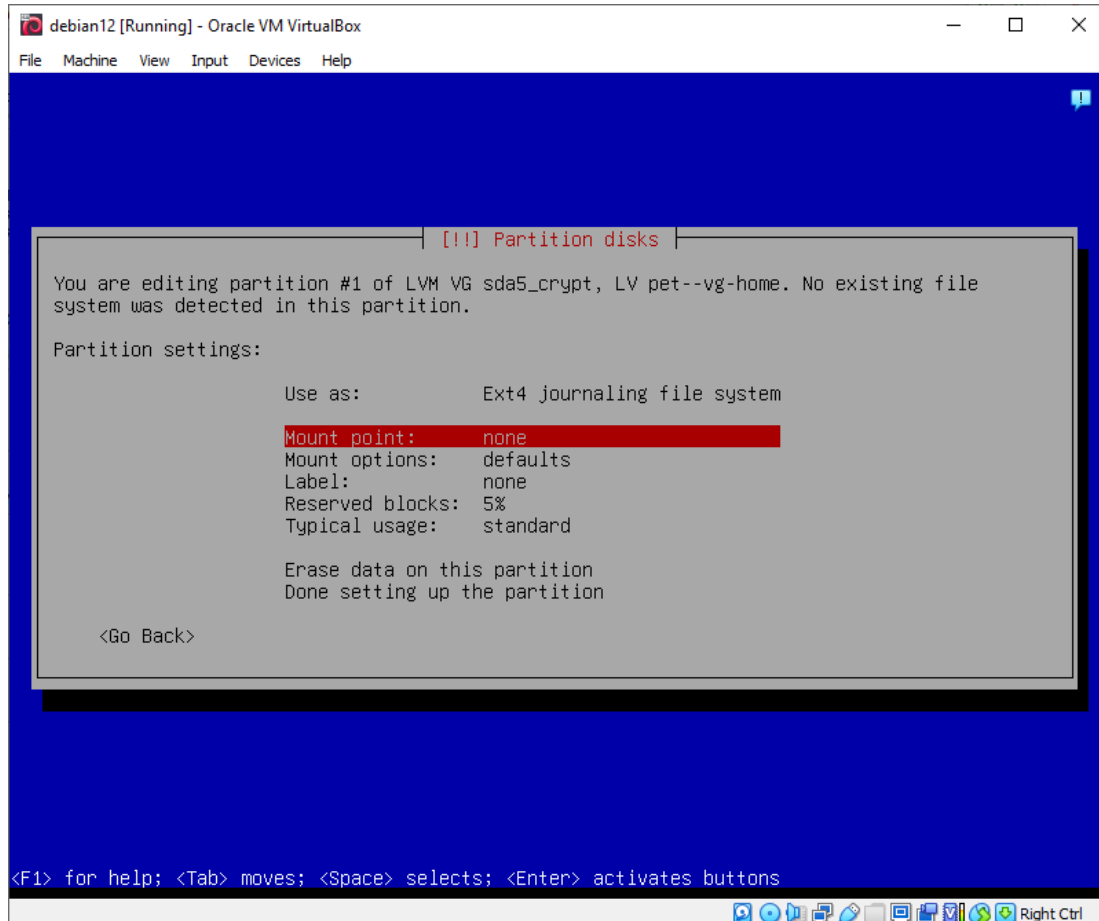


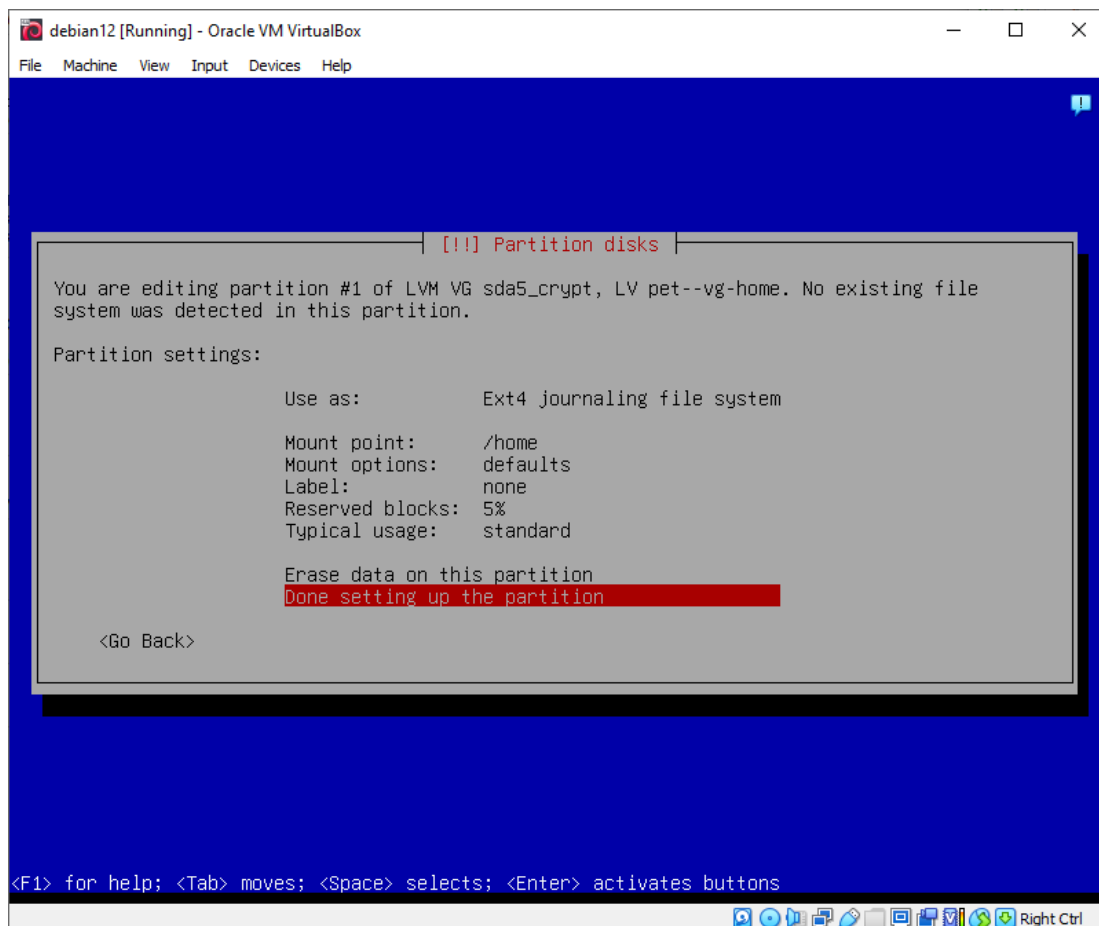
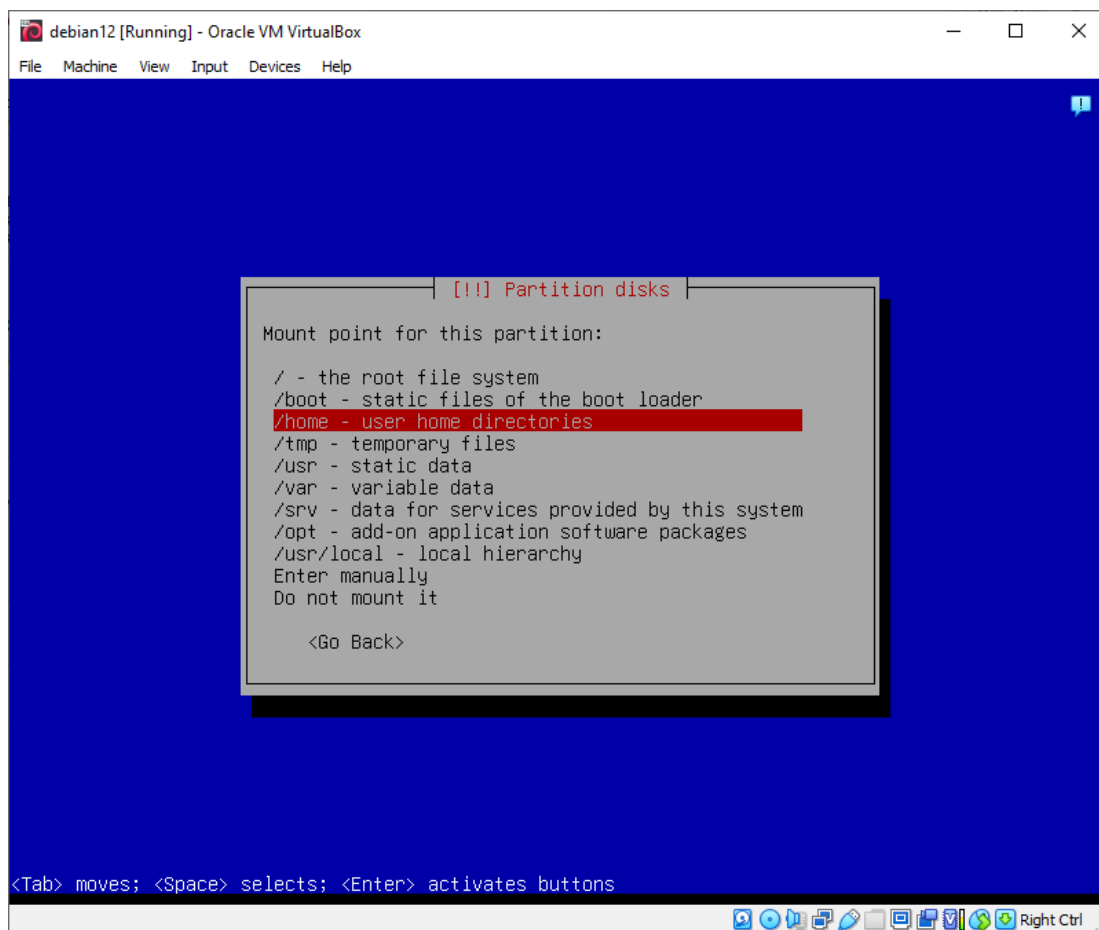






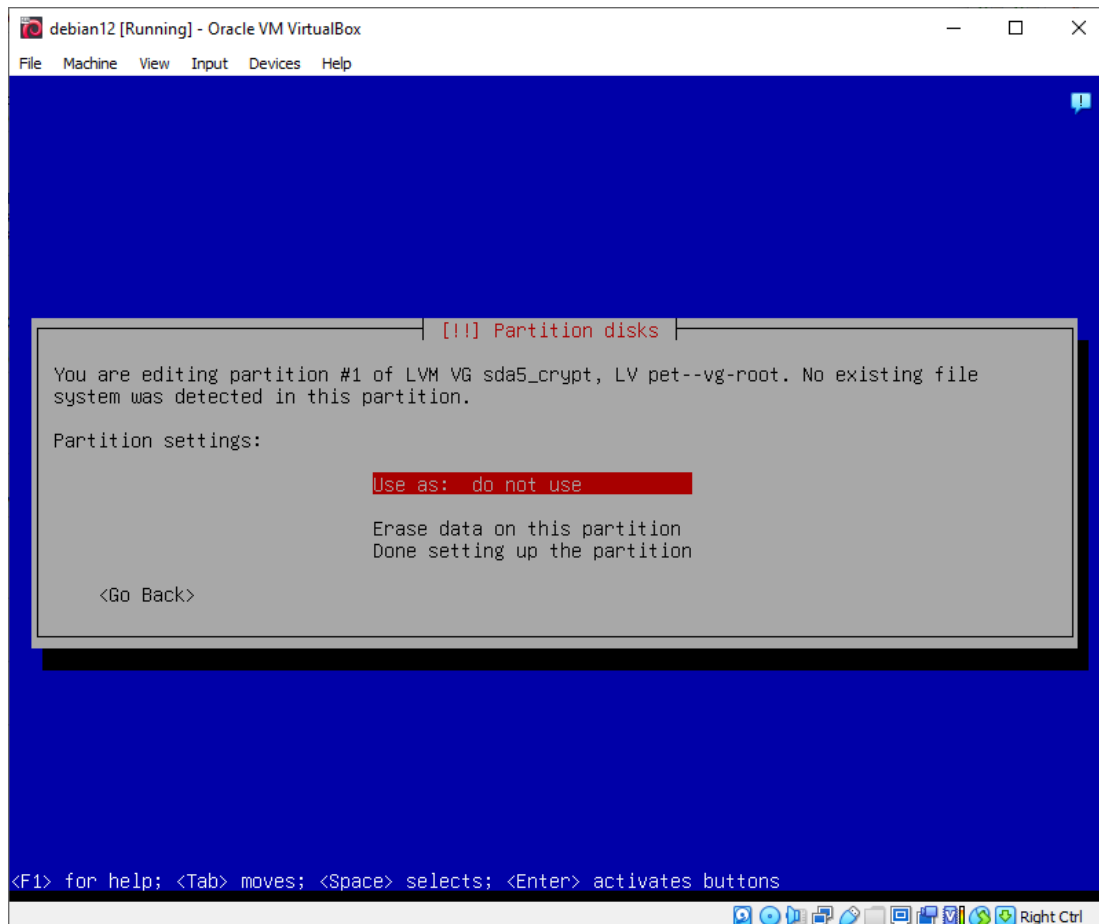
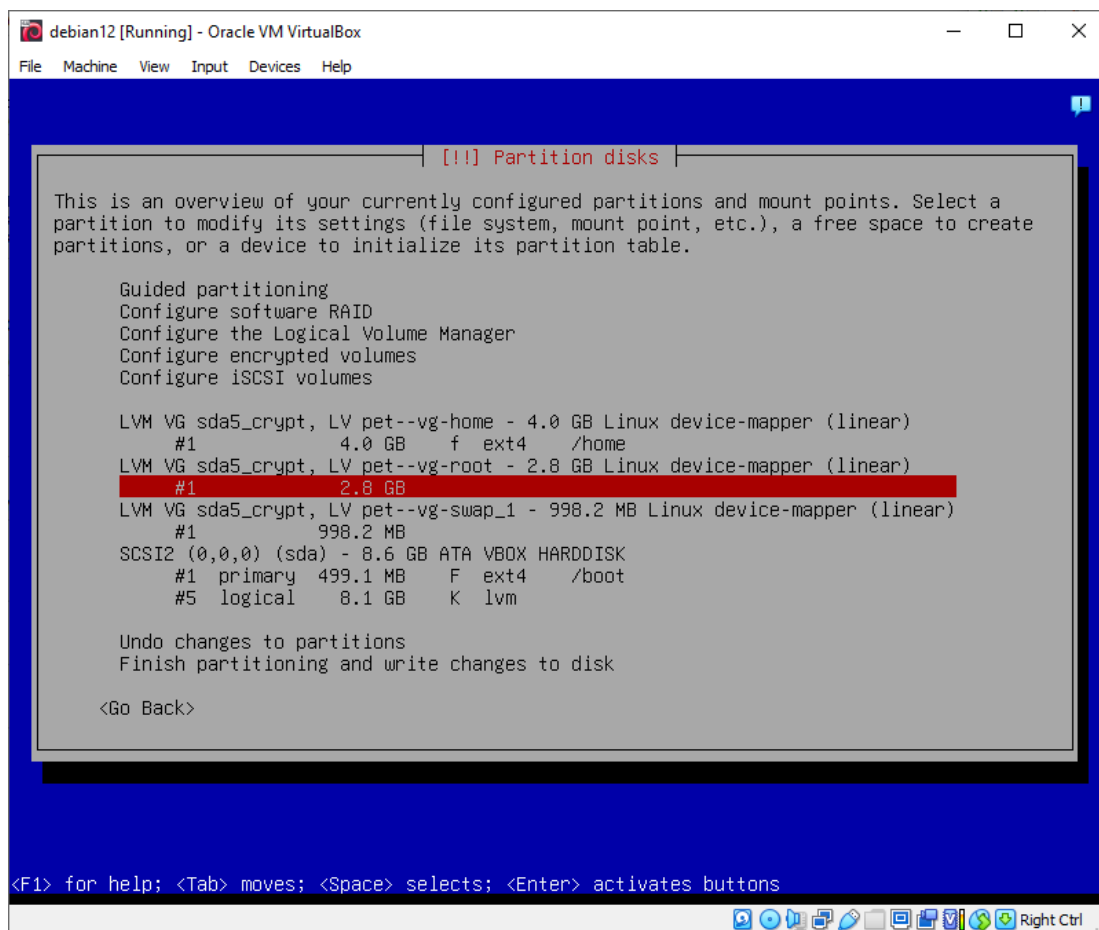
Select Mount Point and set to /home

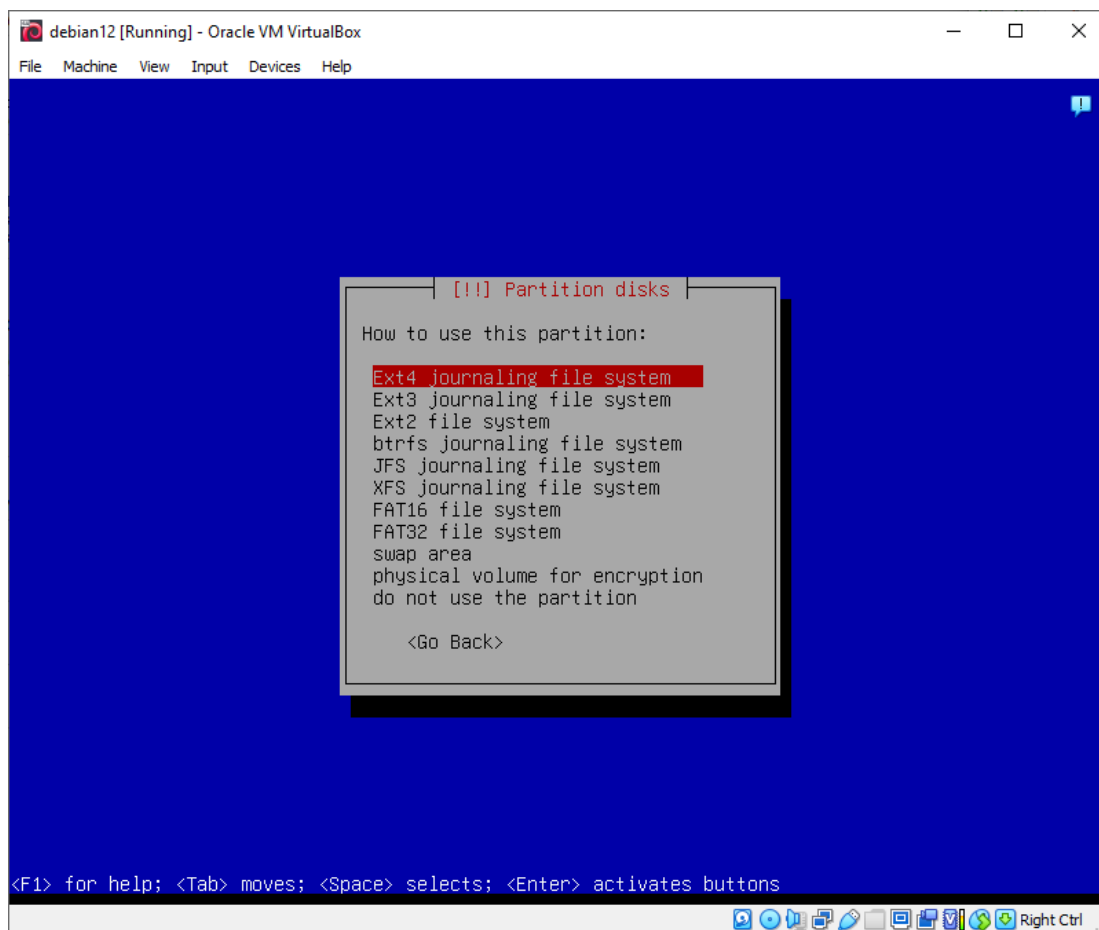




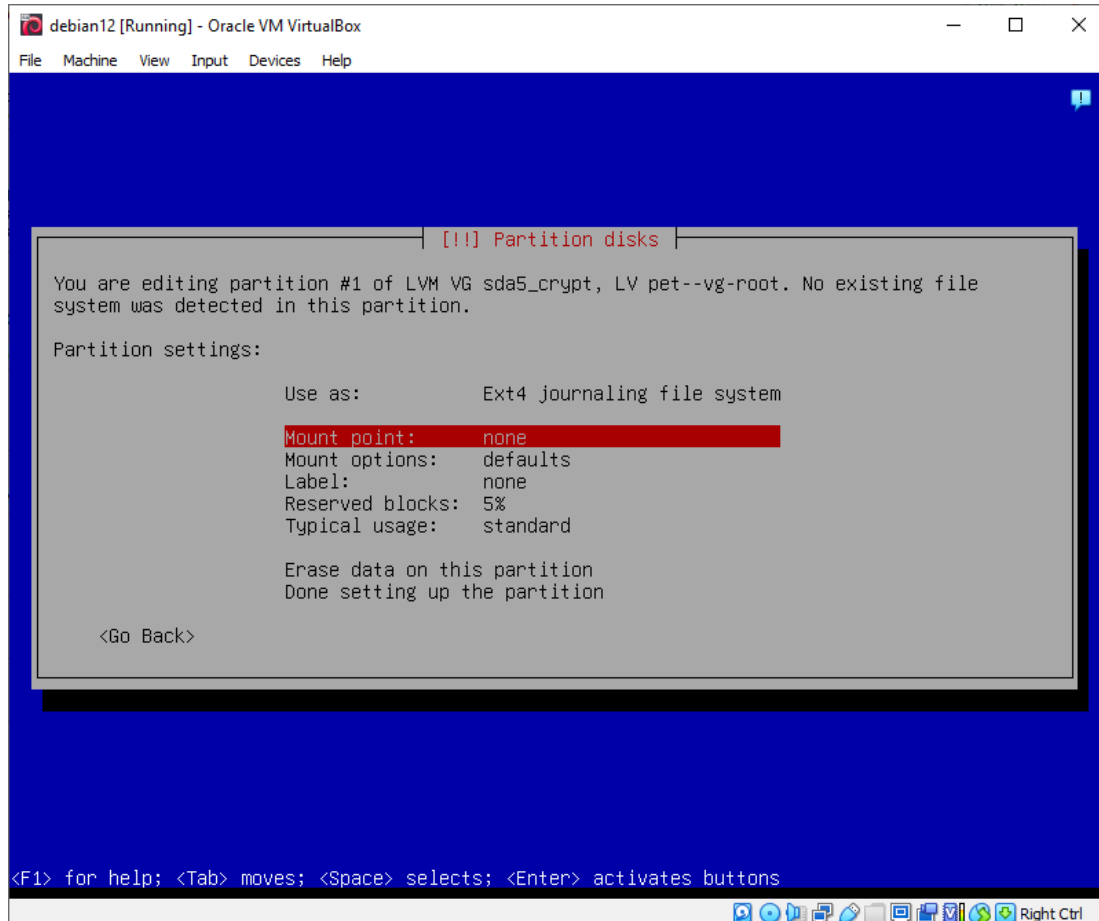
/ (root file system)

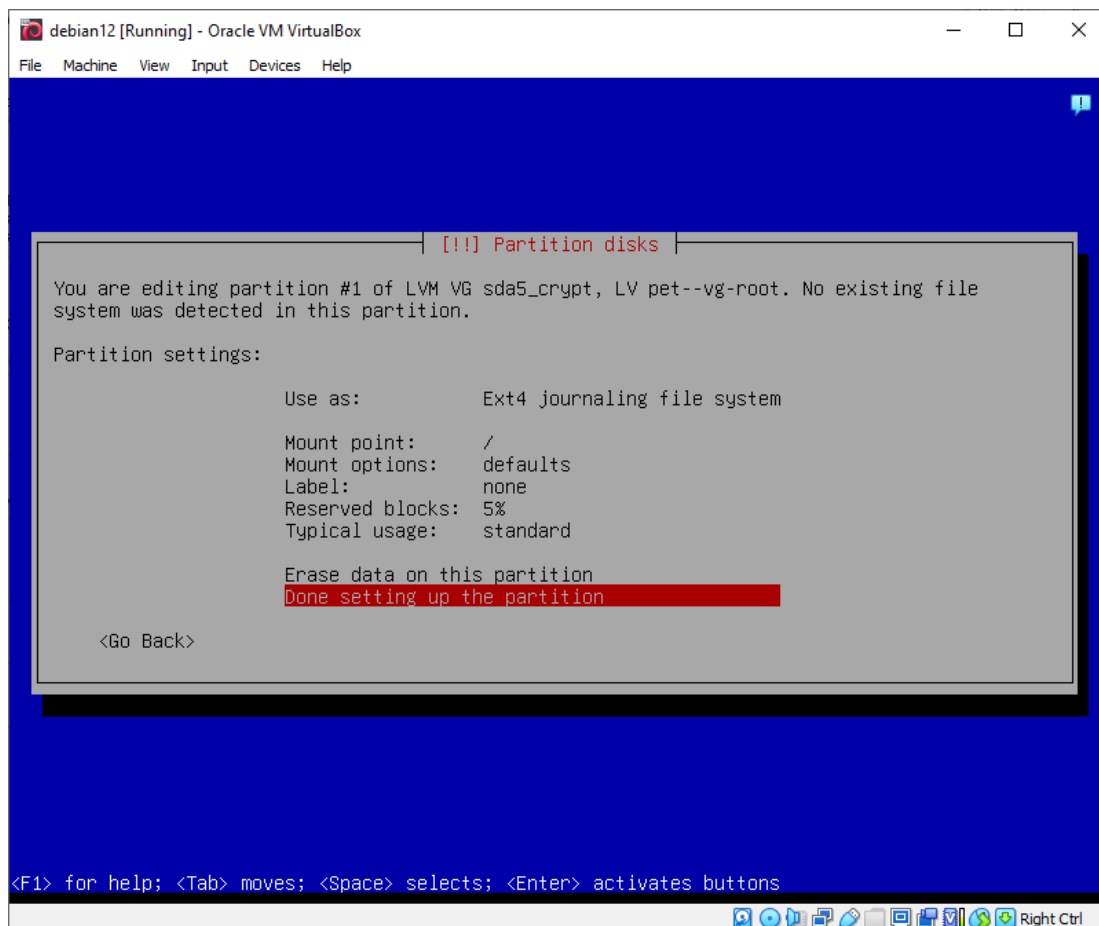
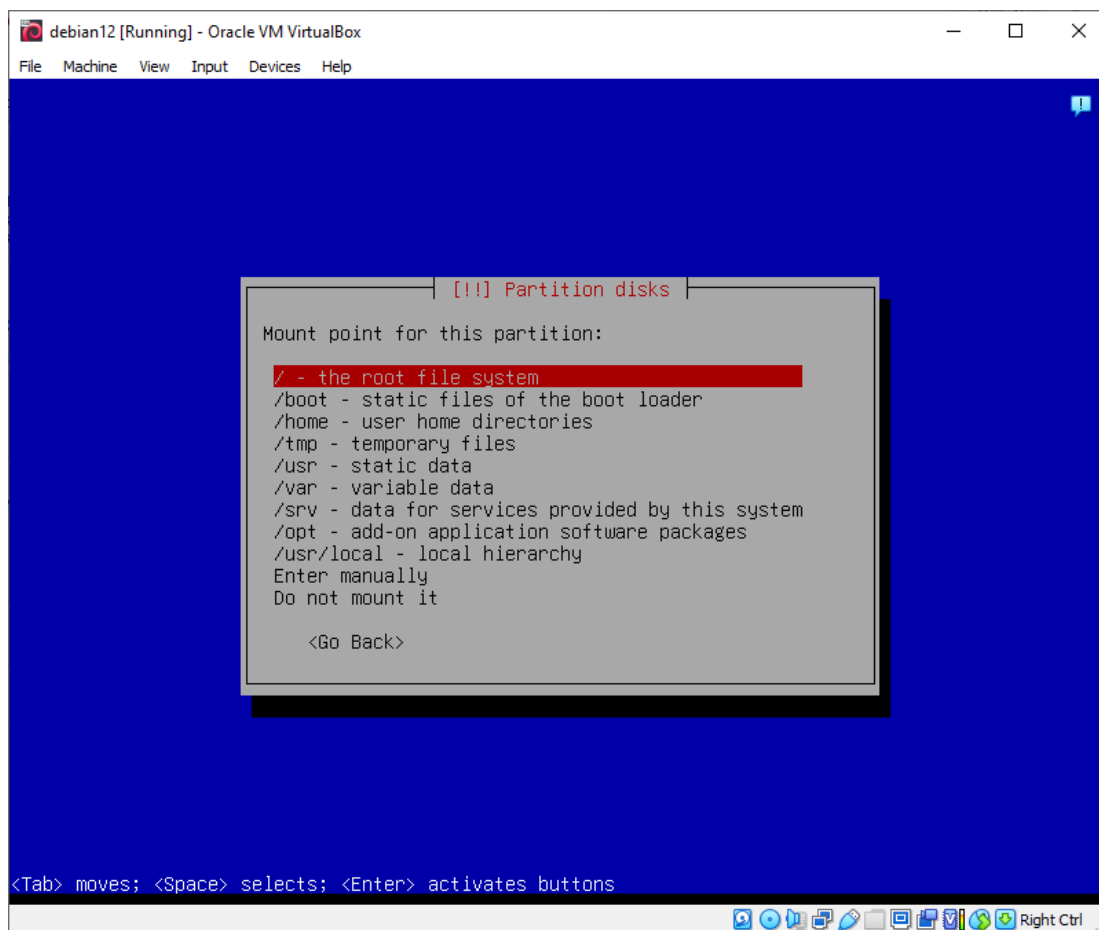


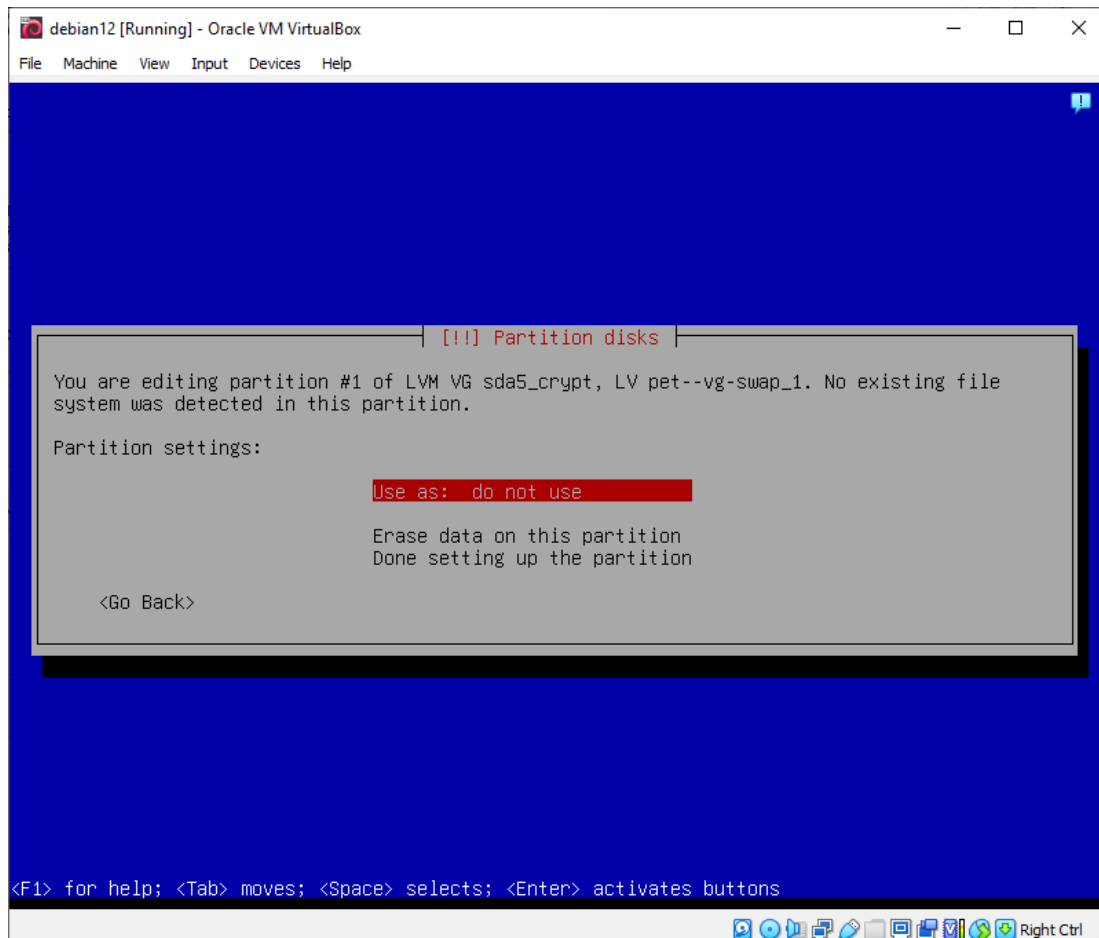
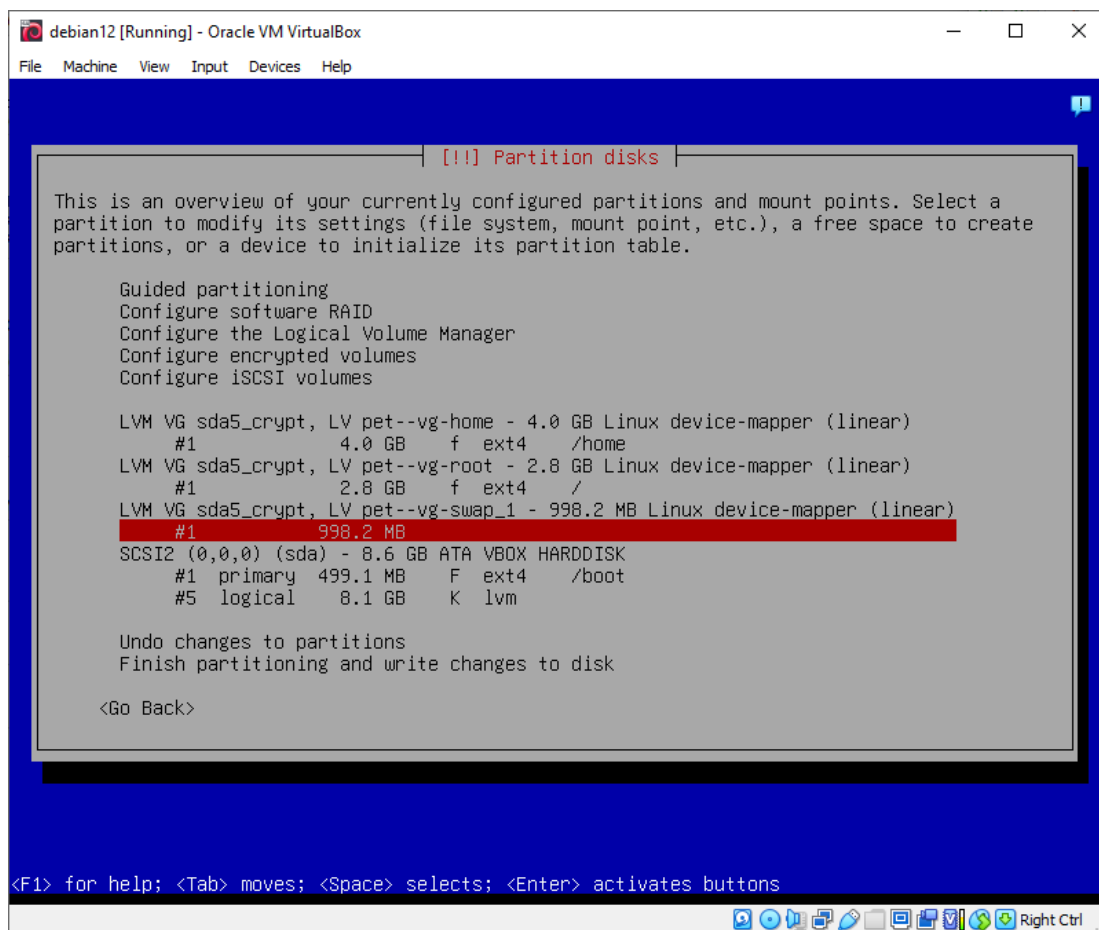


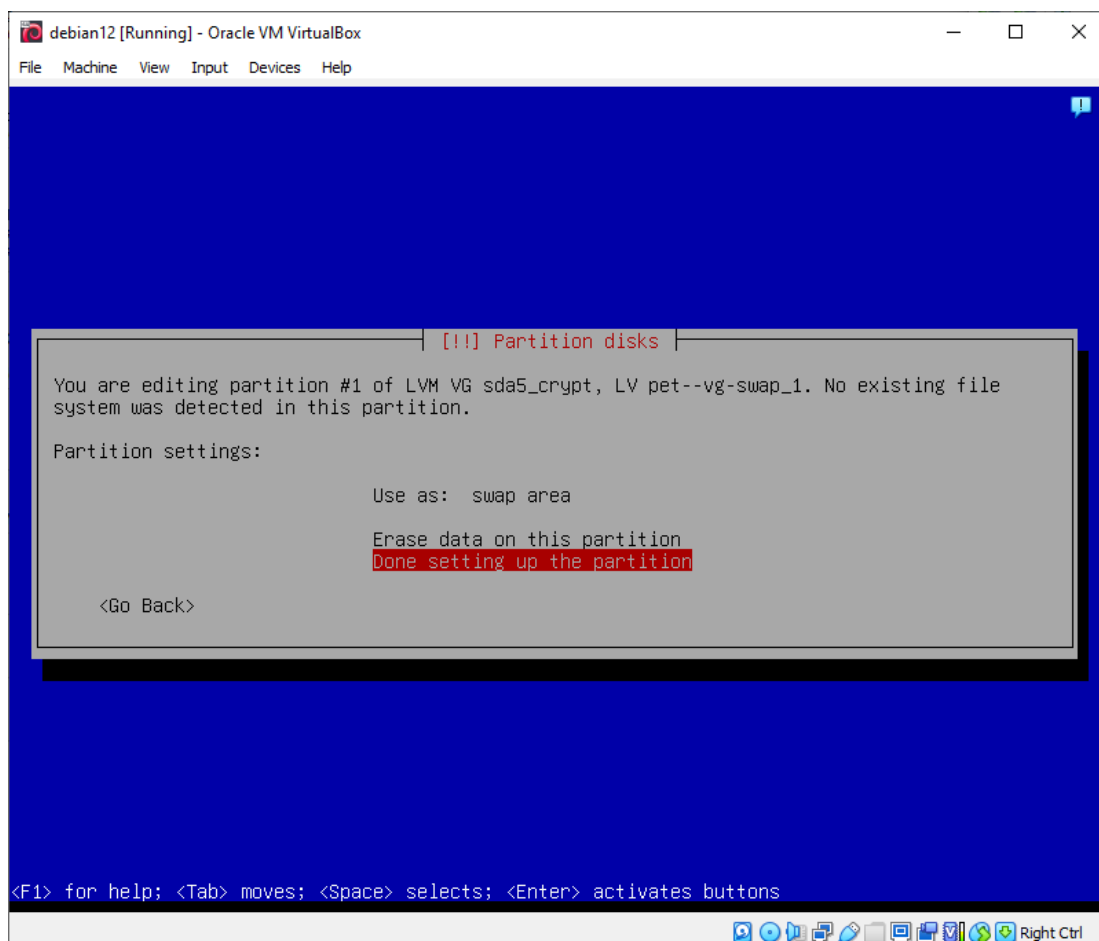
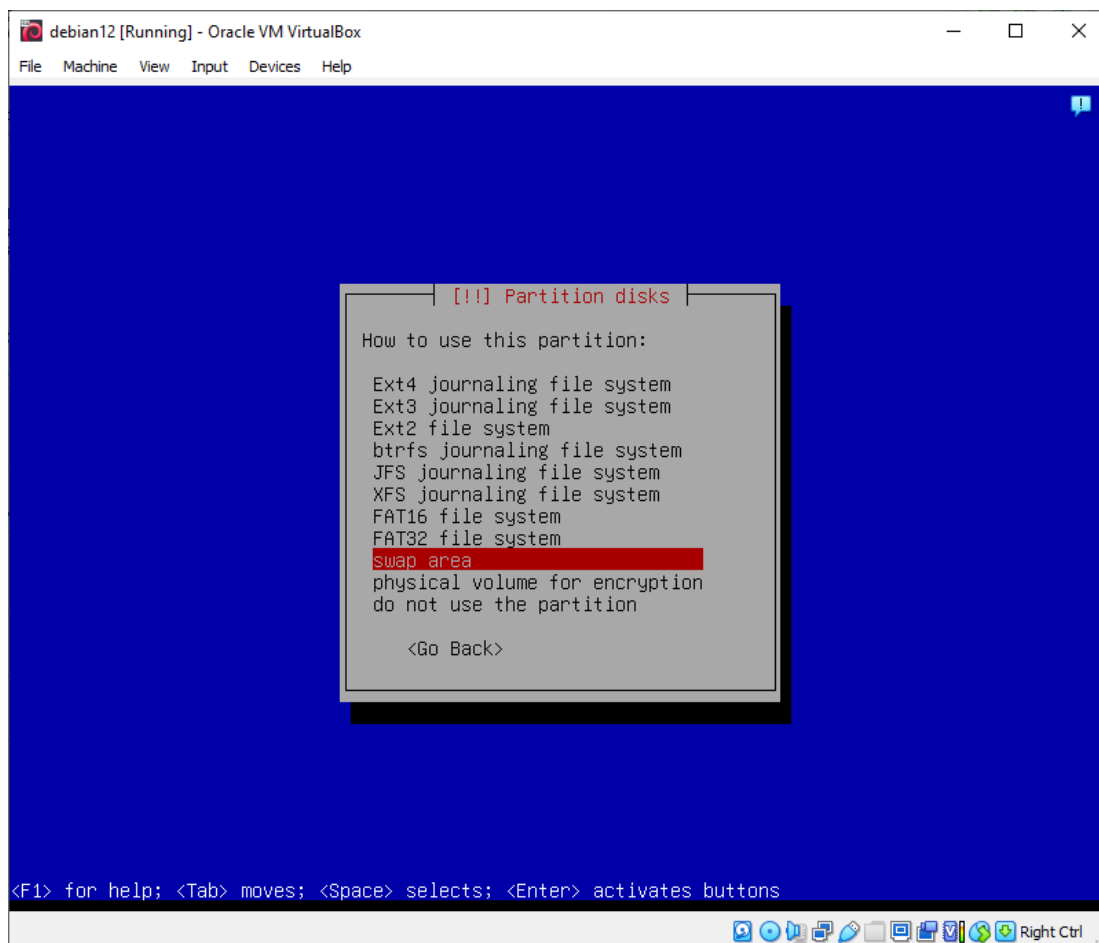


Select Mount point and set as / (root file system)

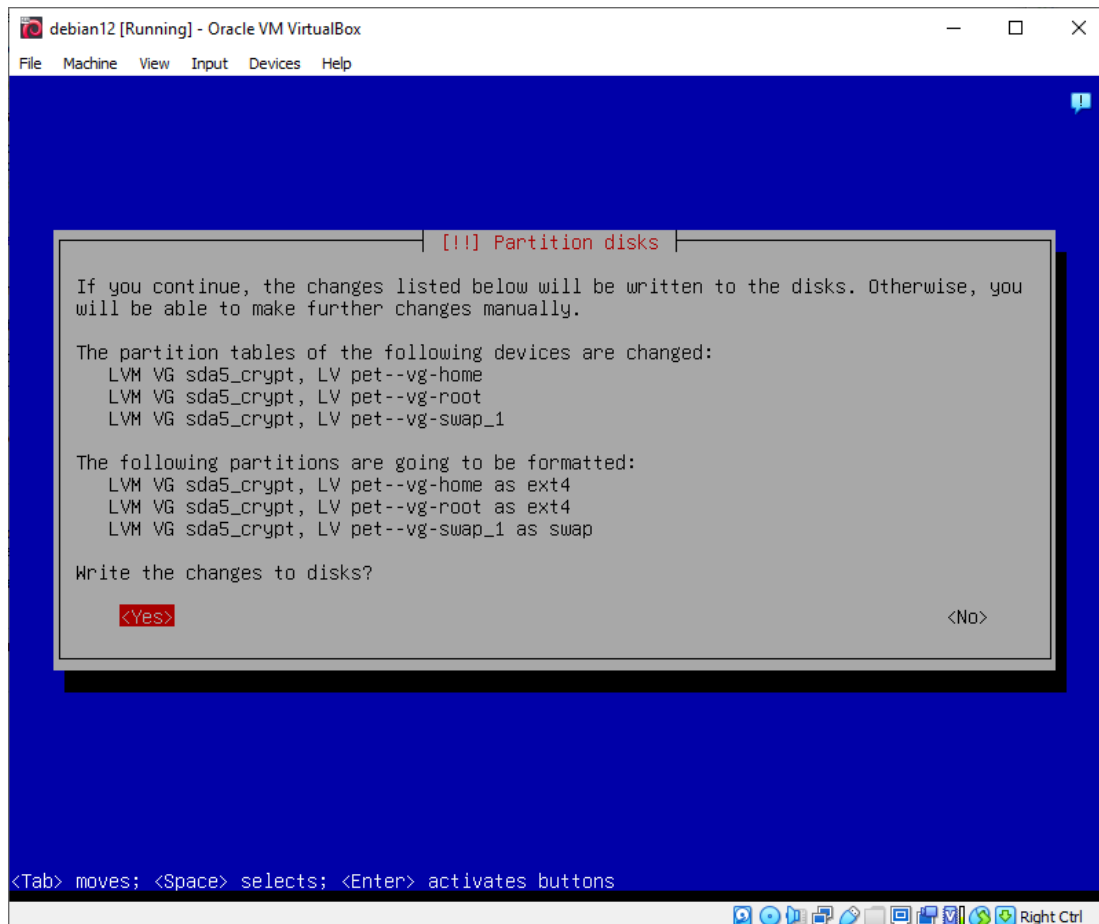
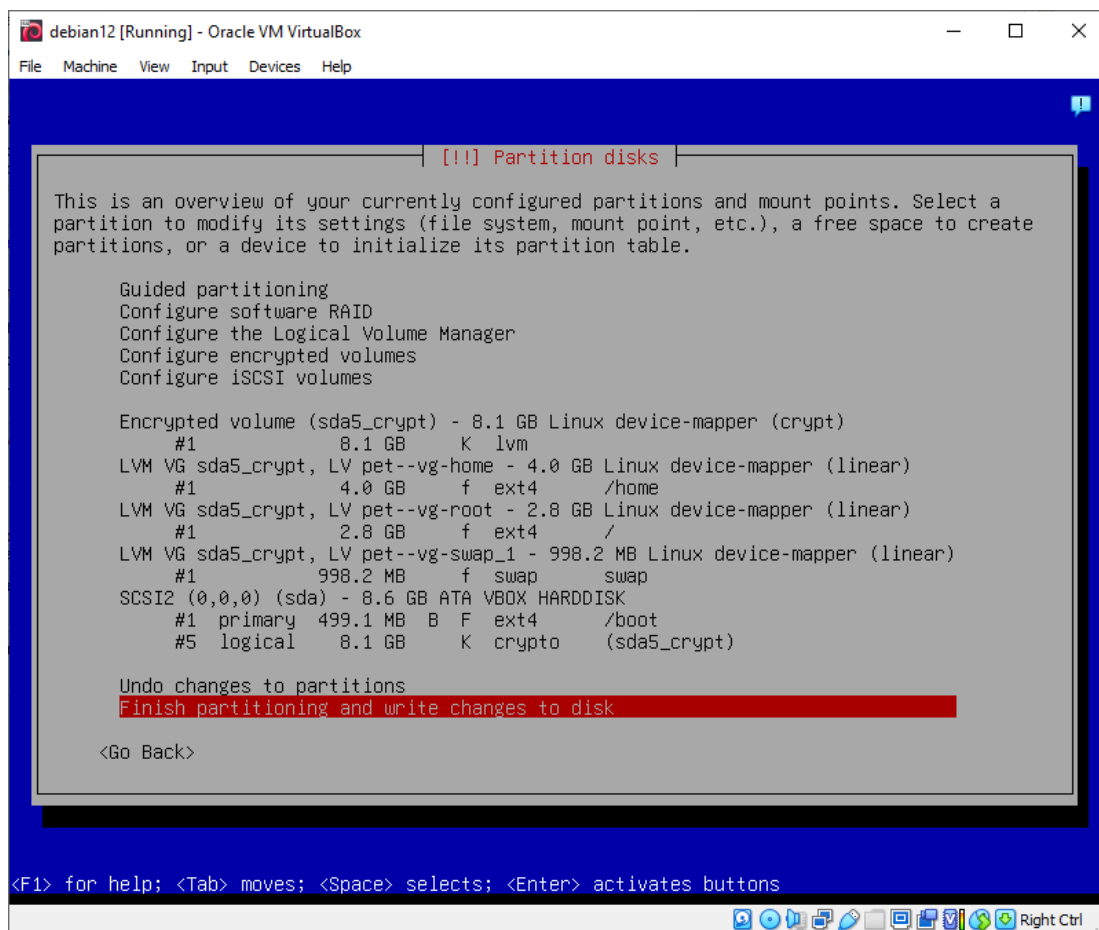


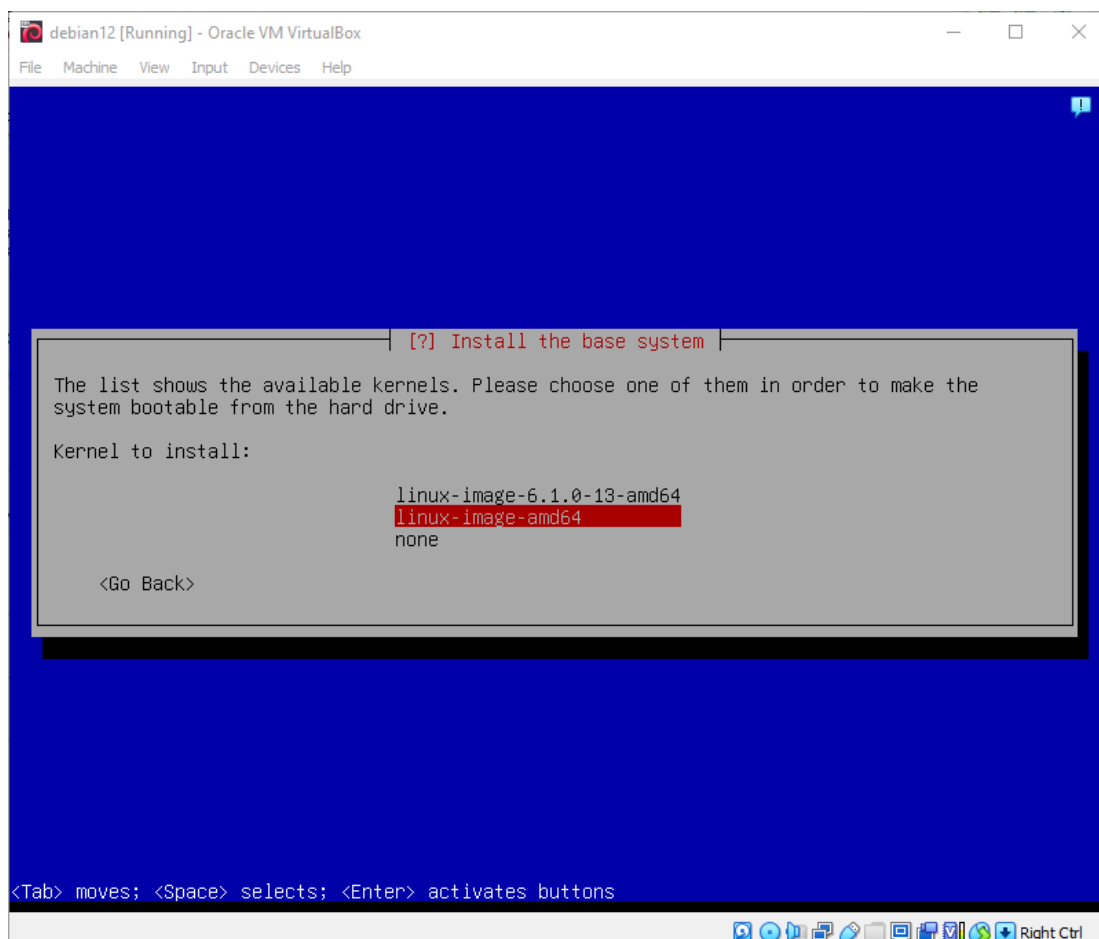
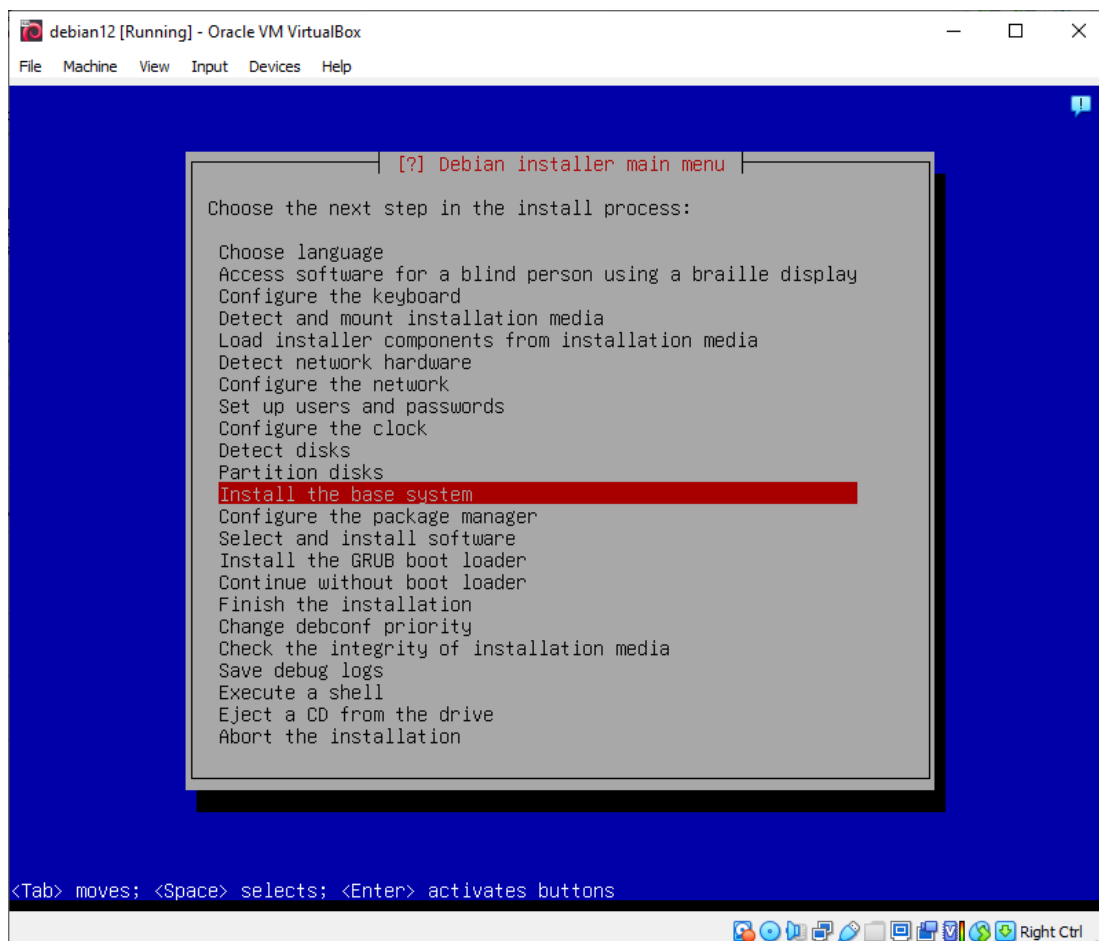


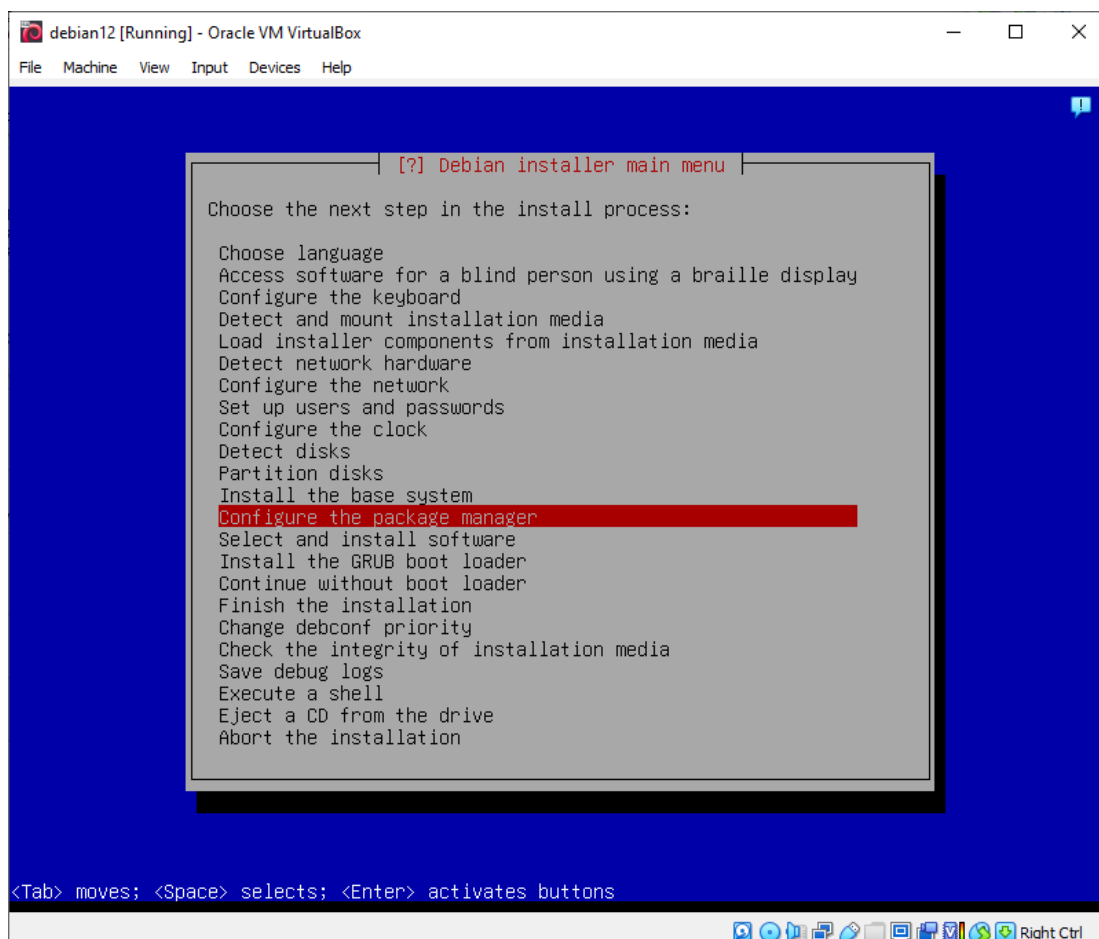
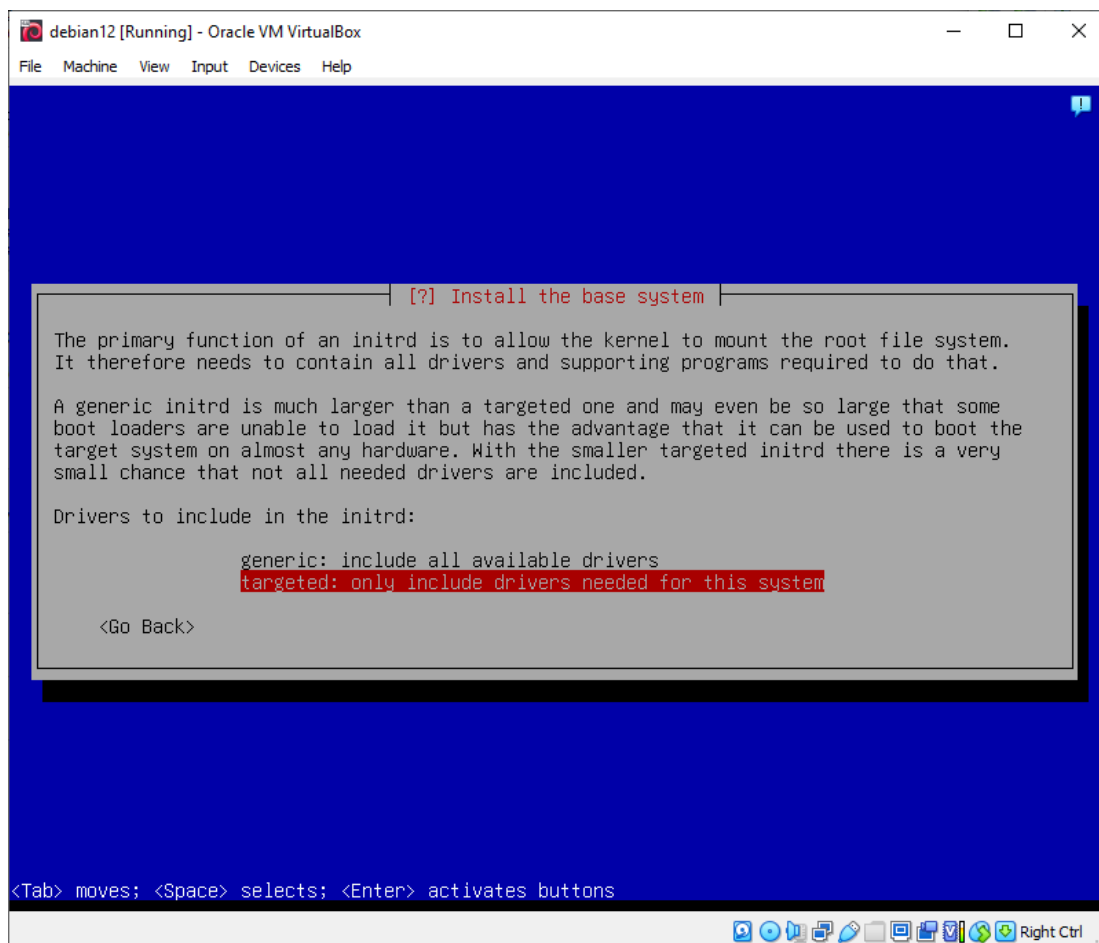




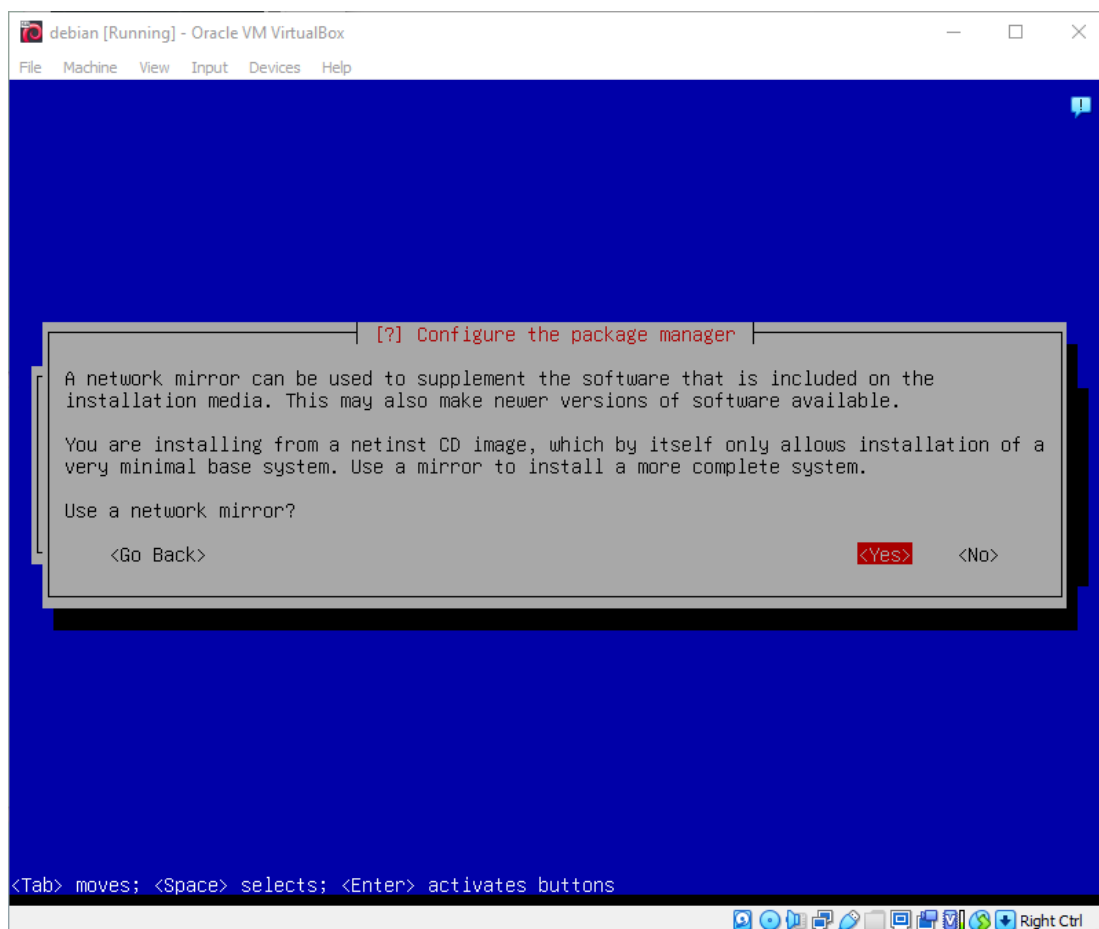
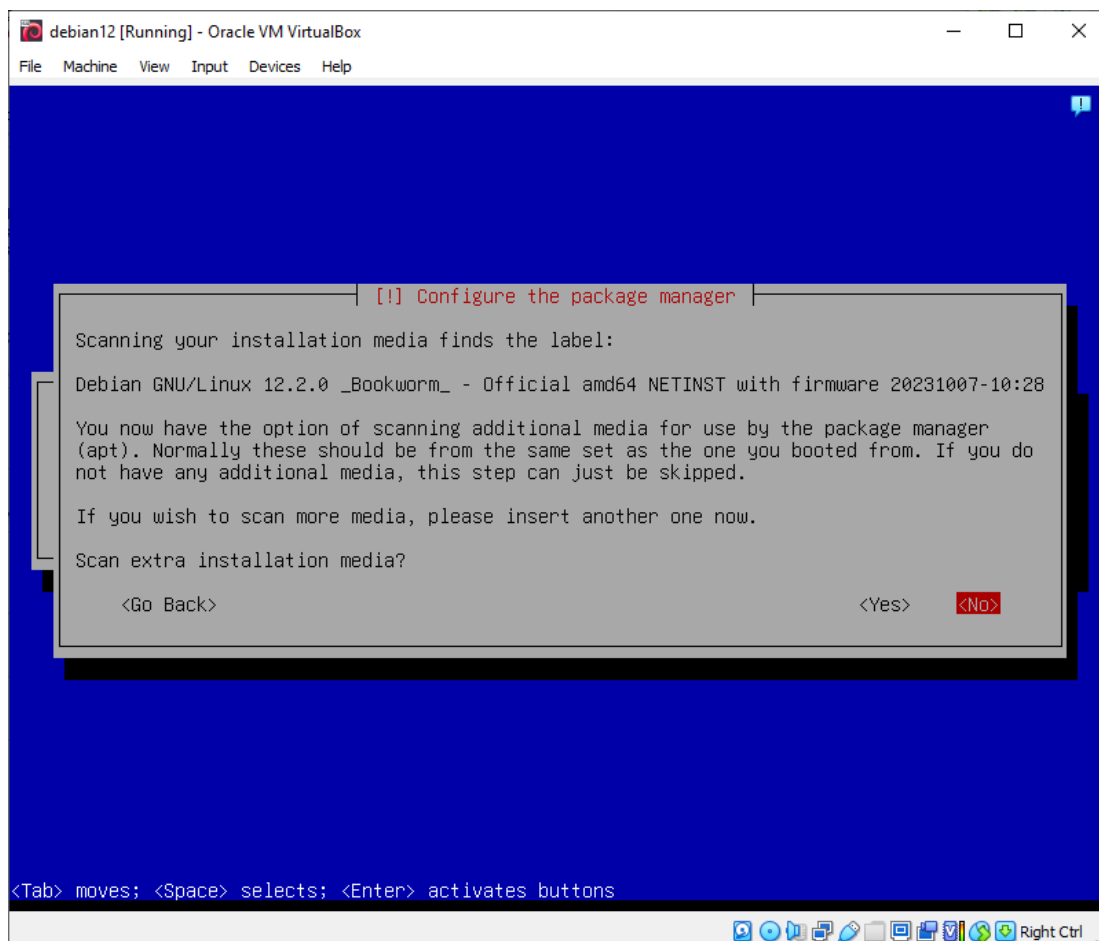
Write partition info to the disk

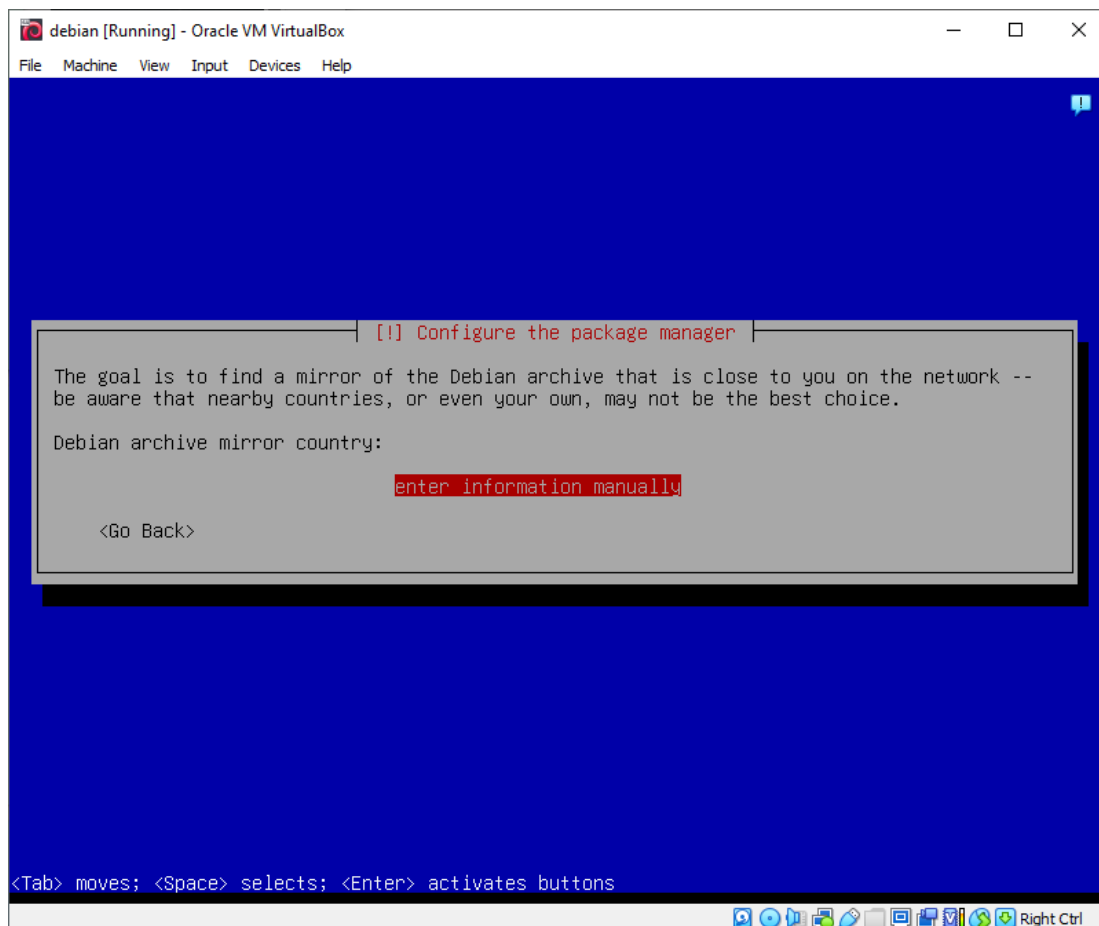
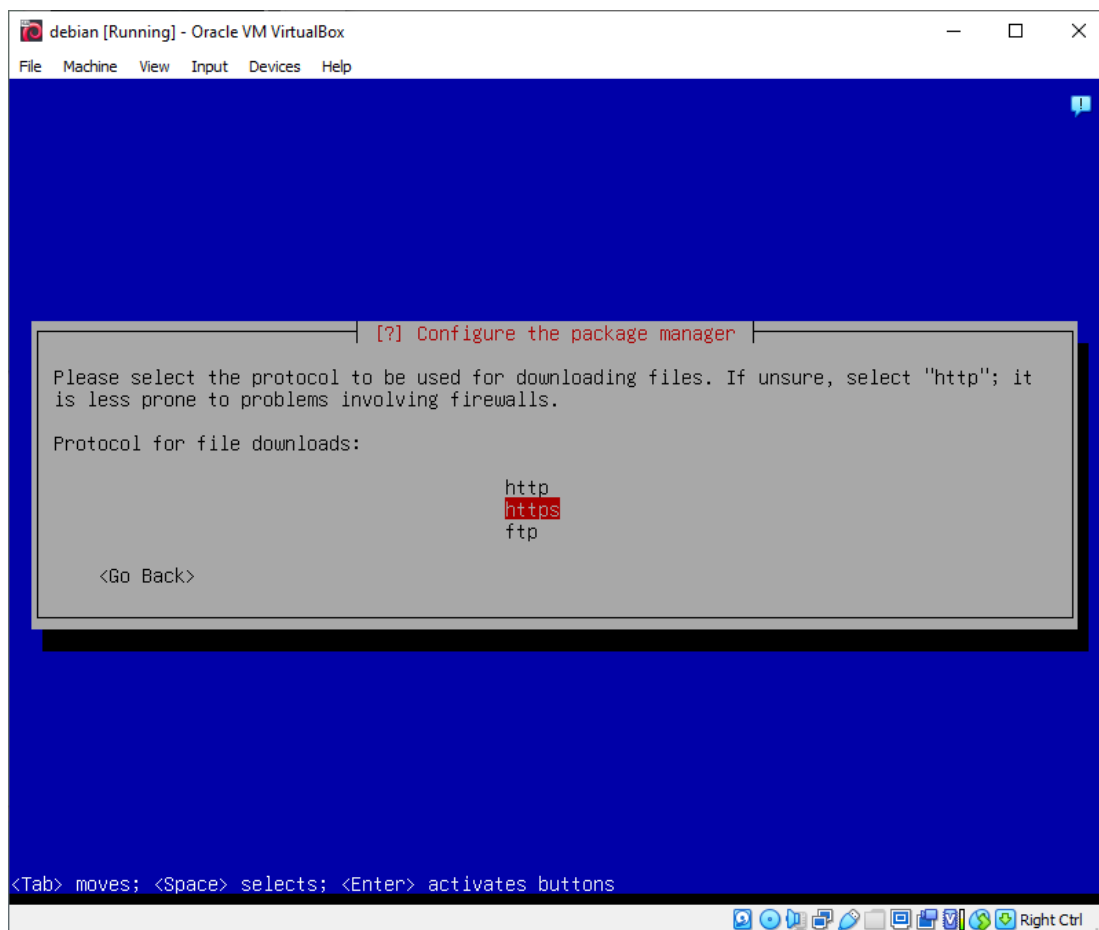


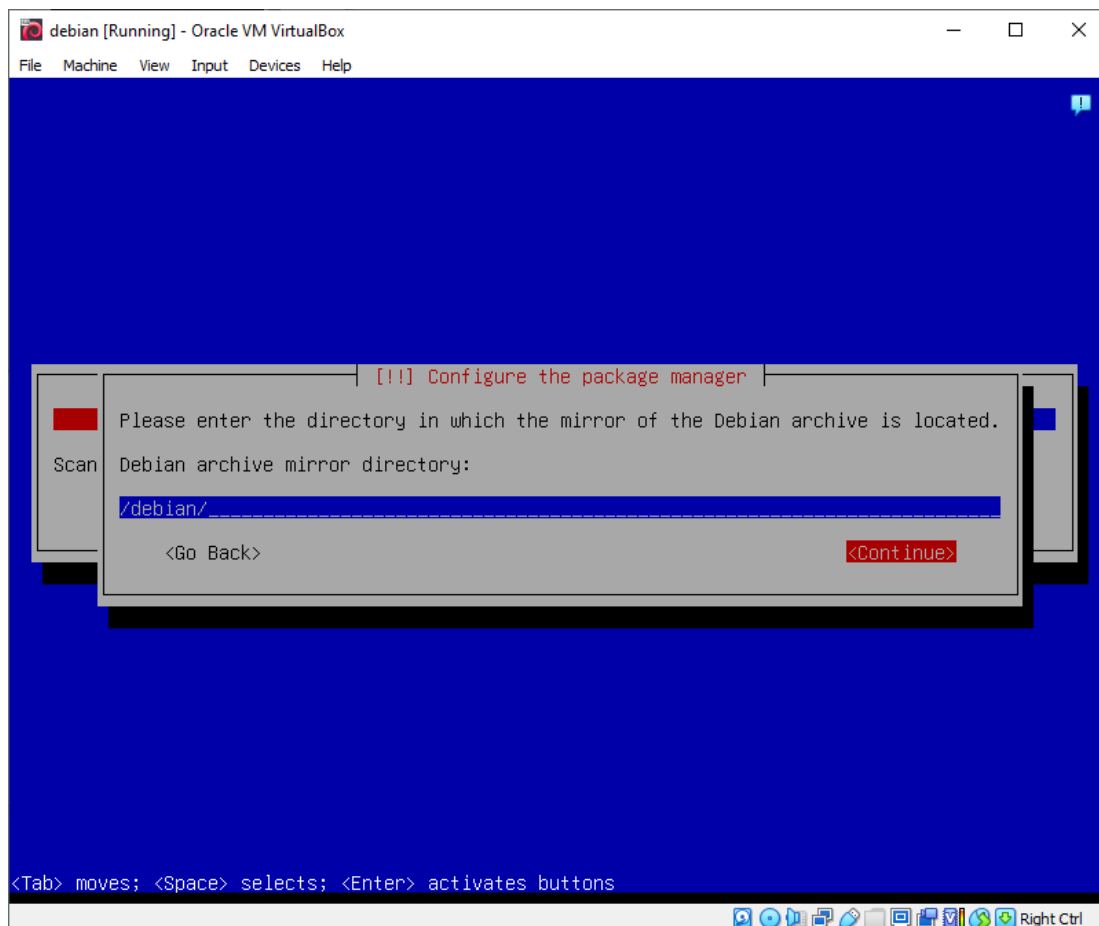
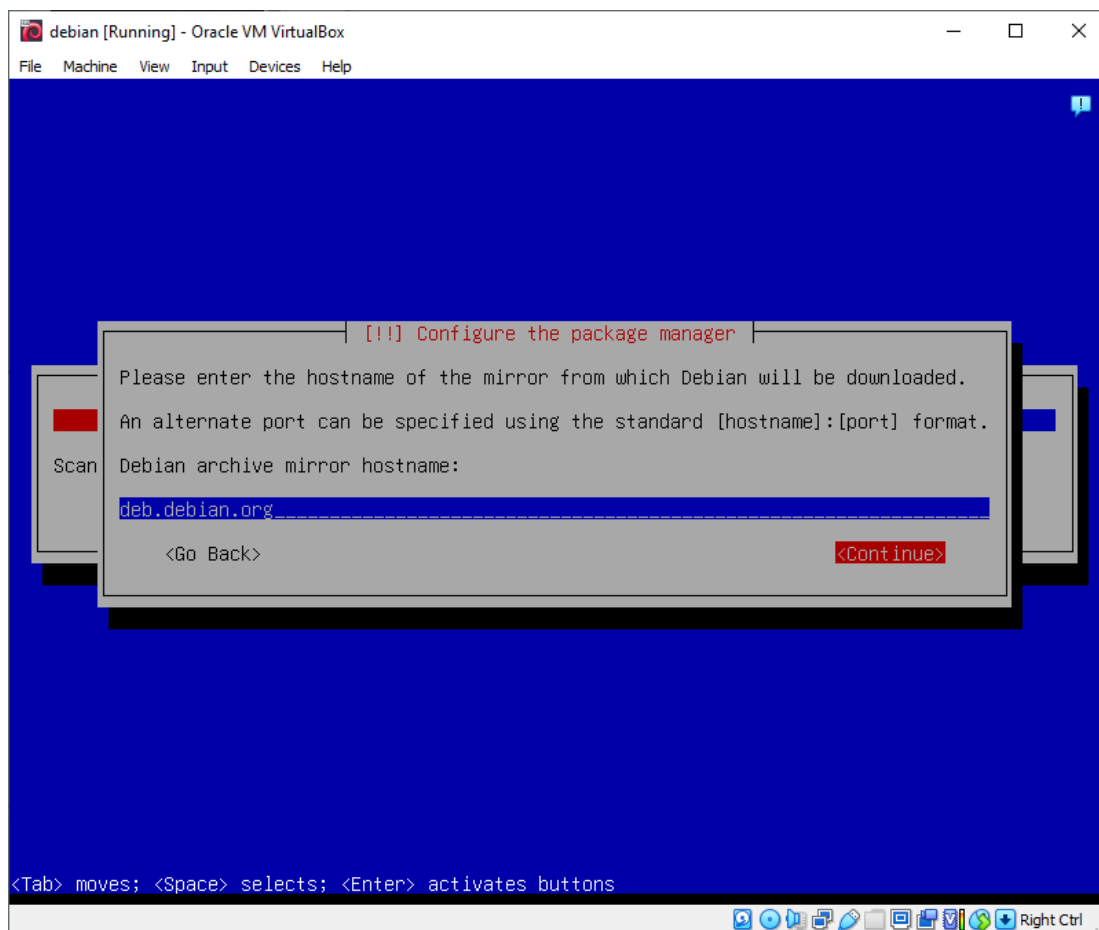


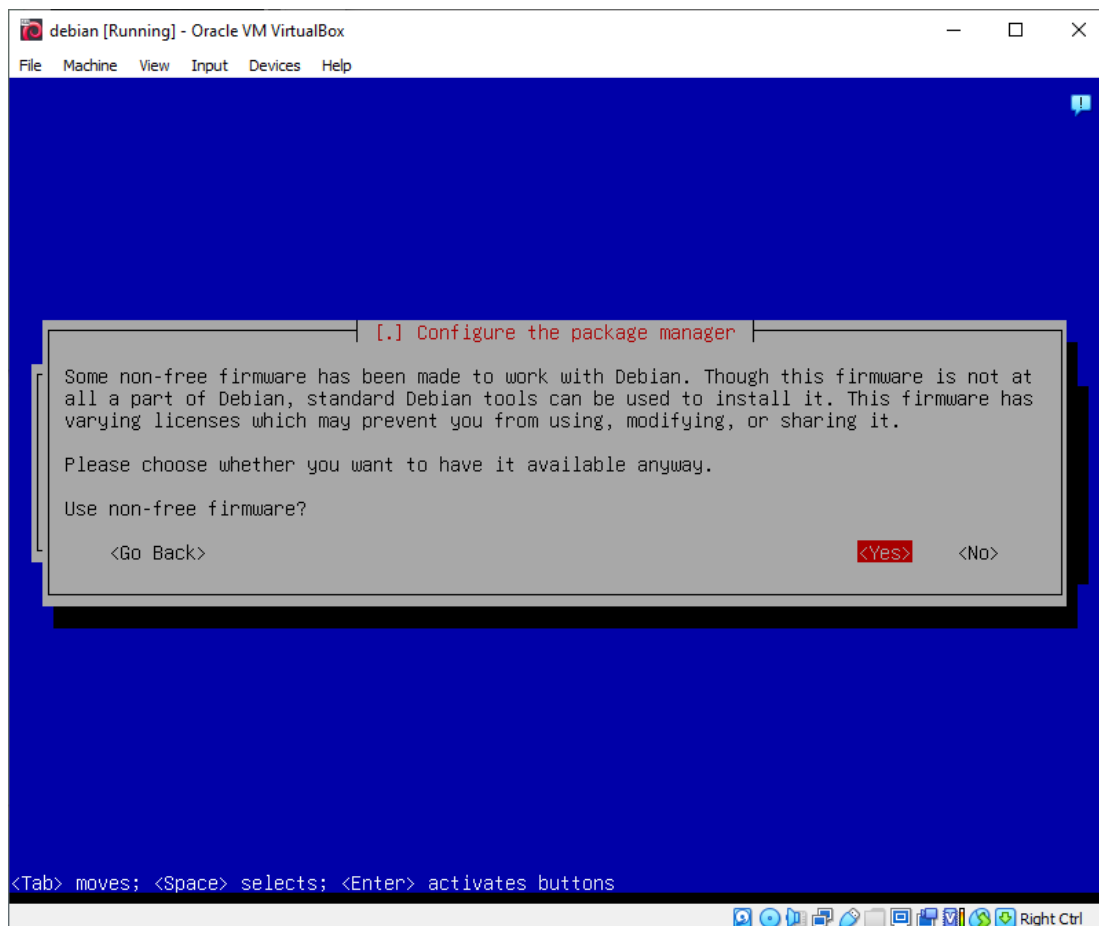
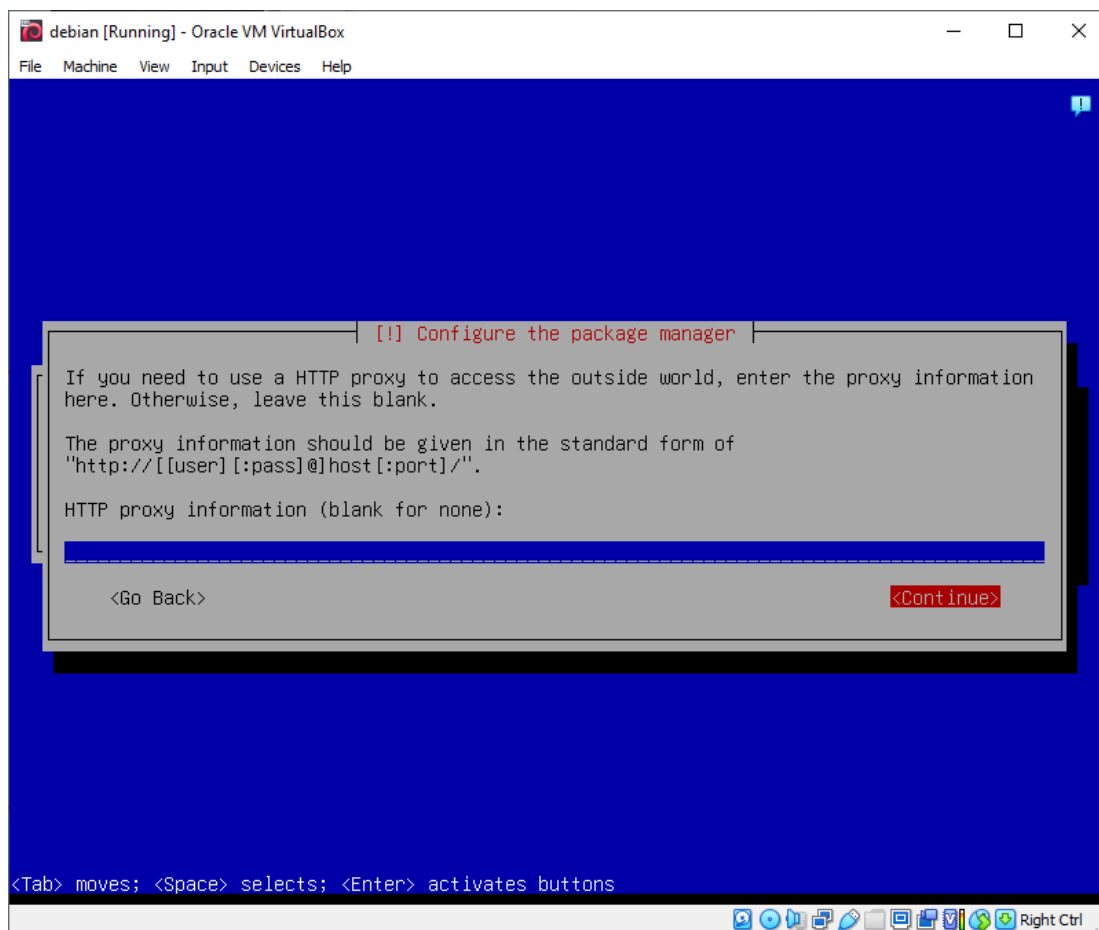


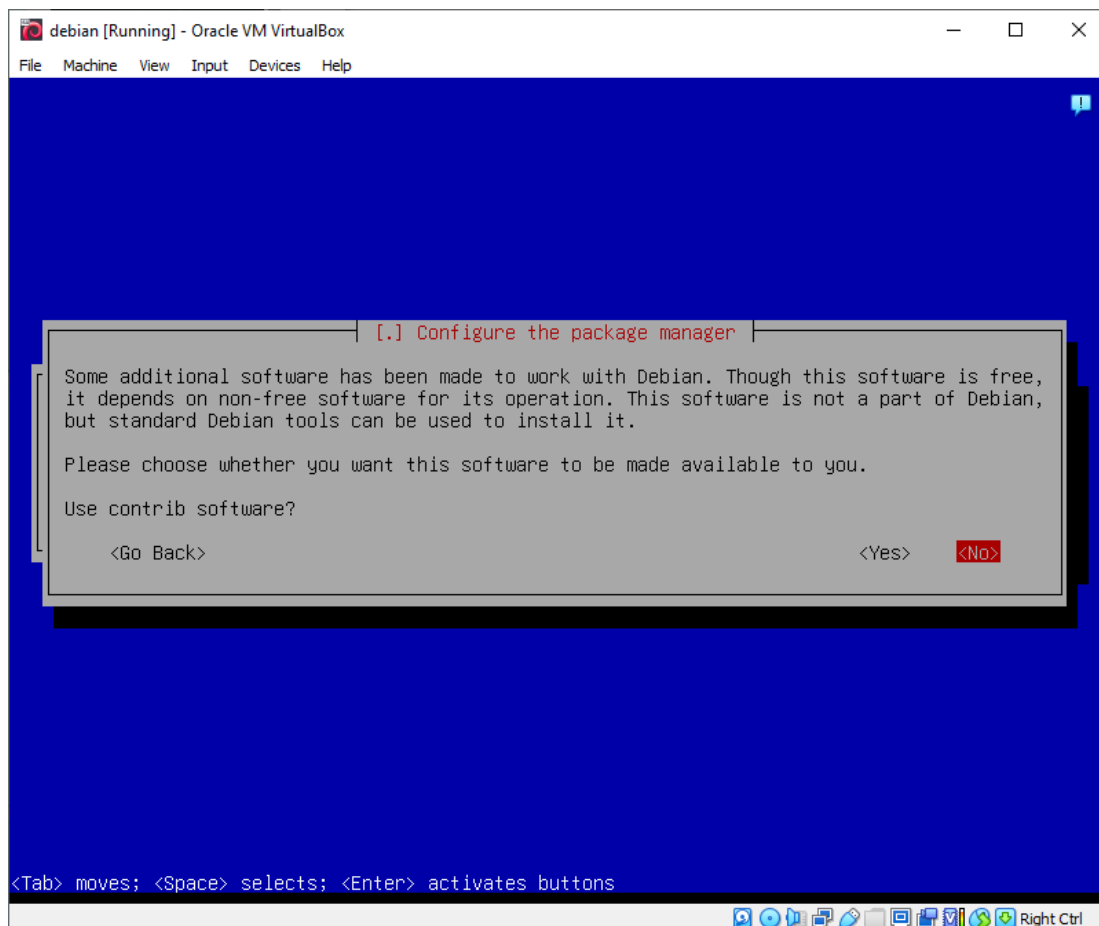
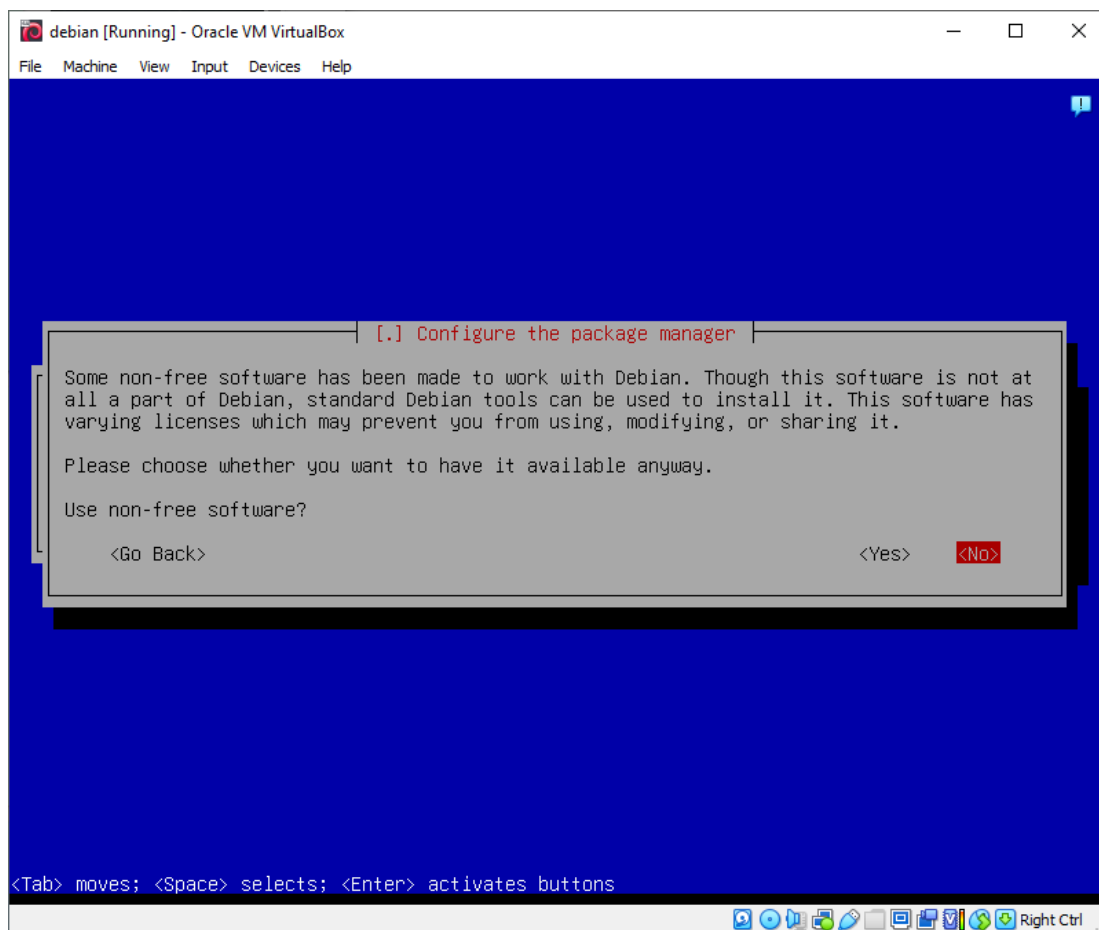


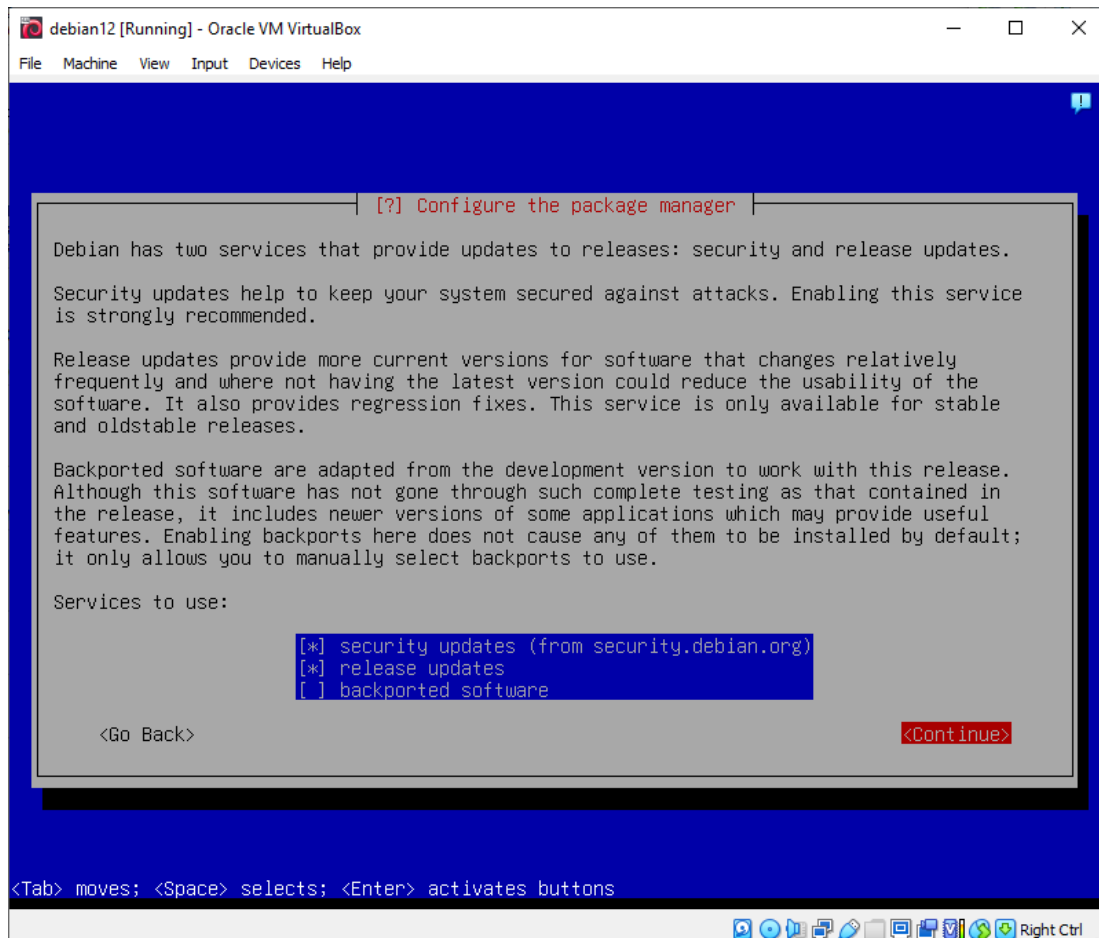
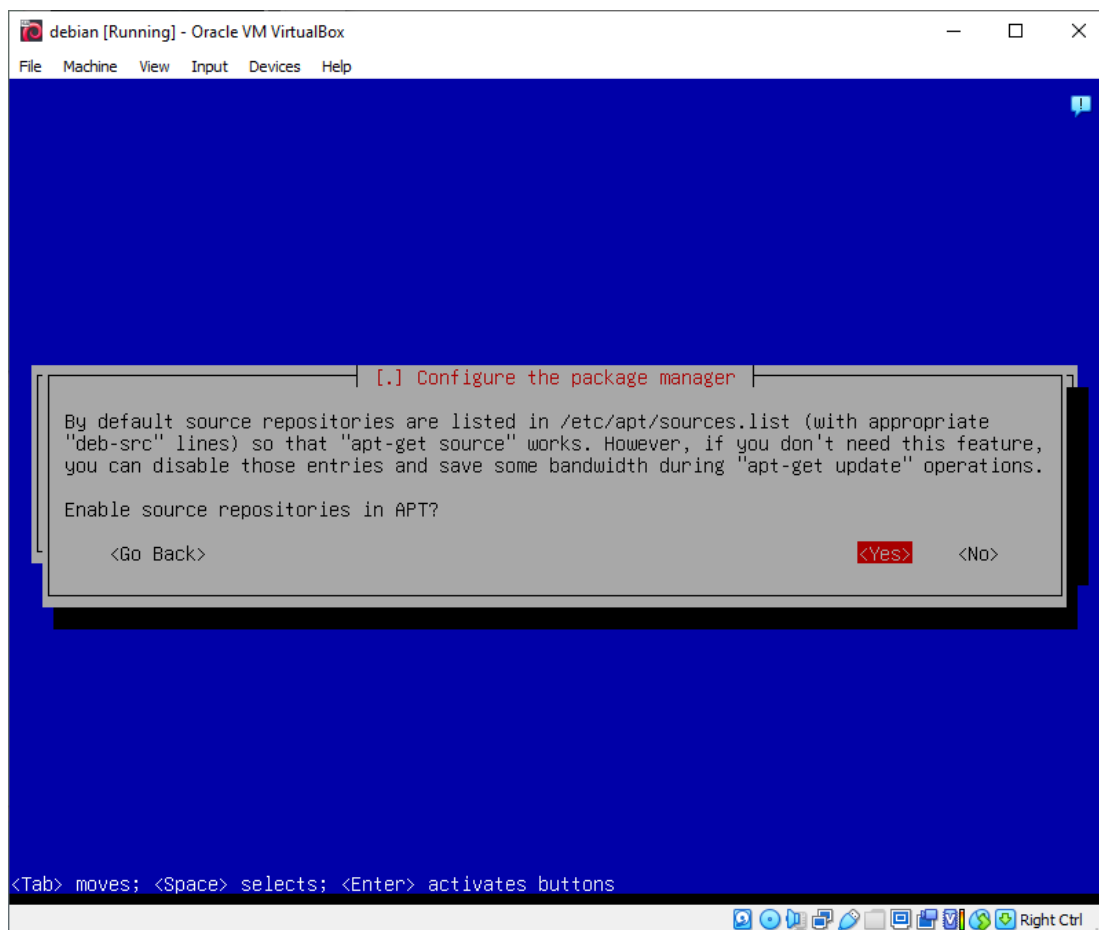


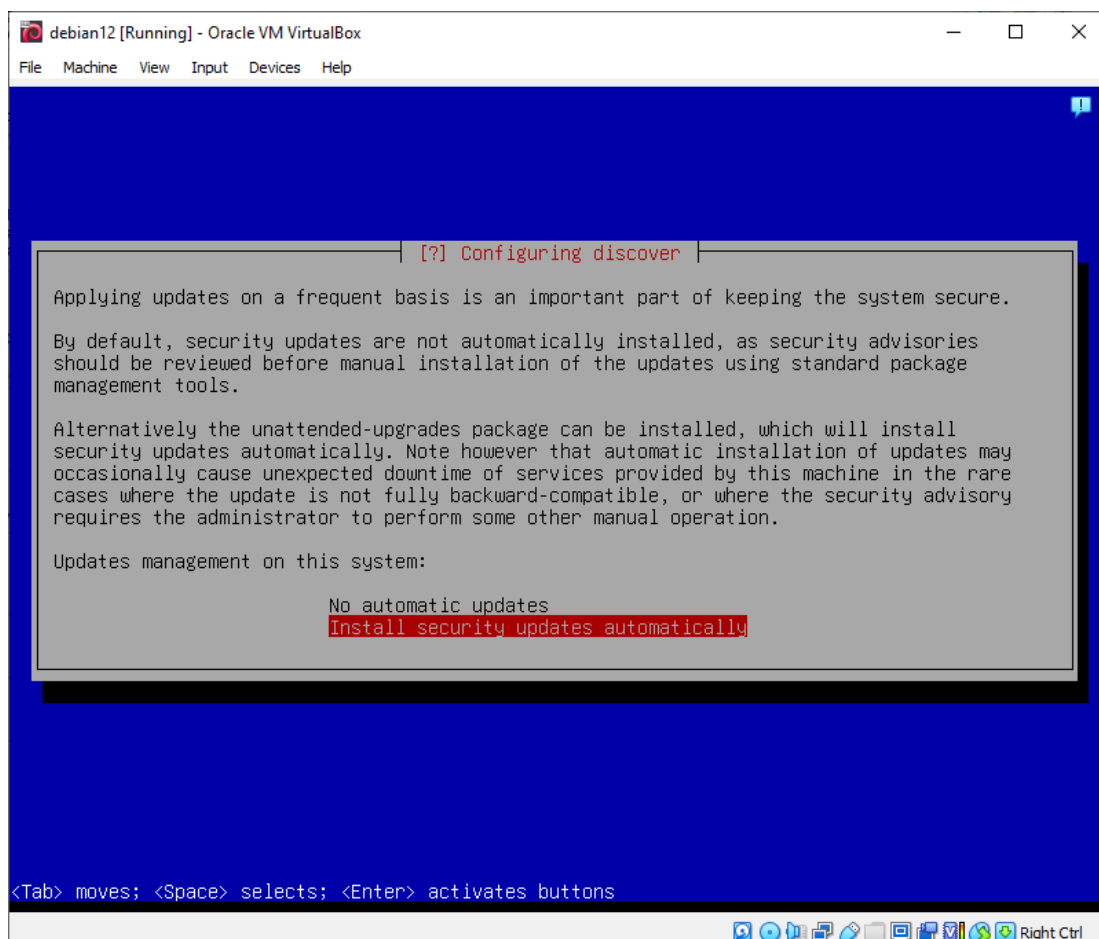
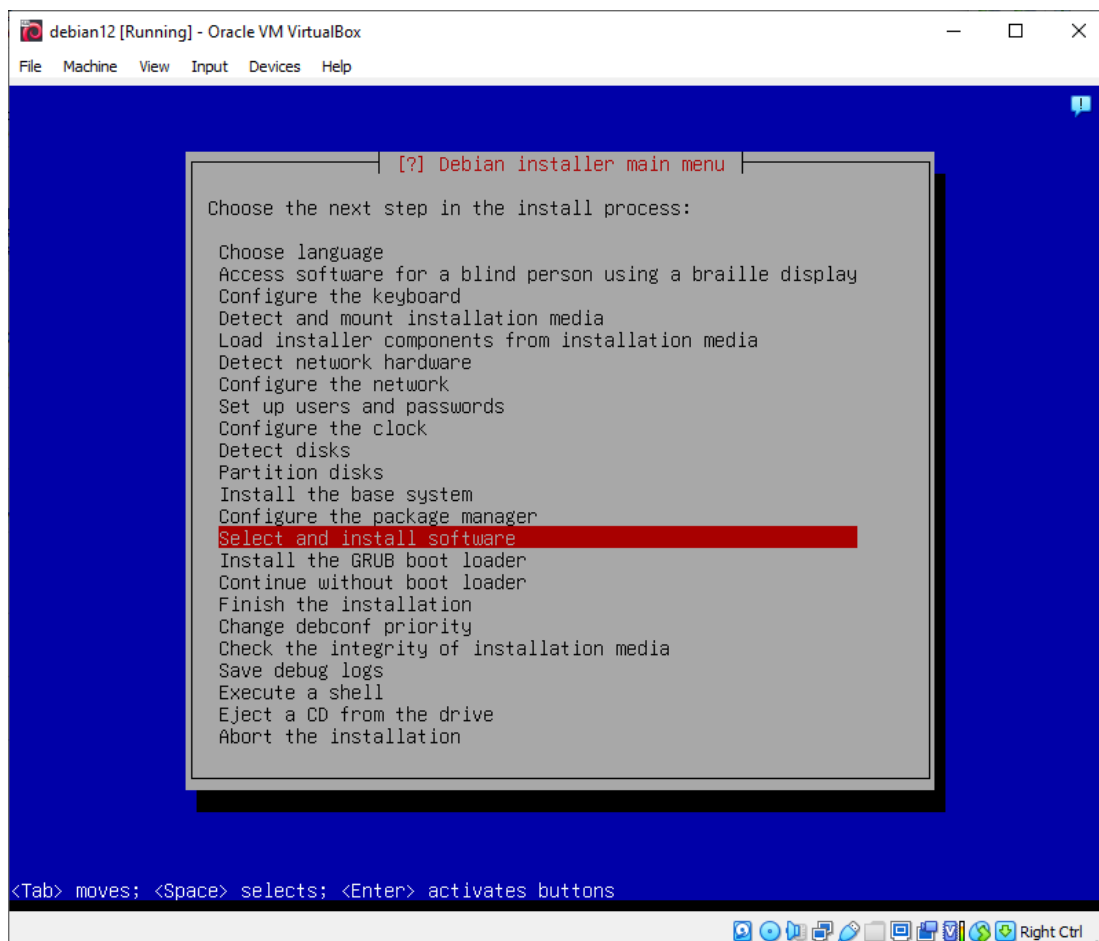


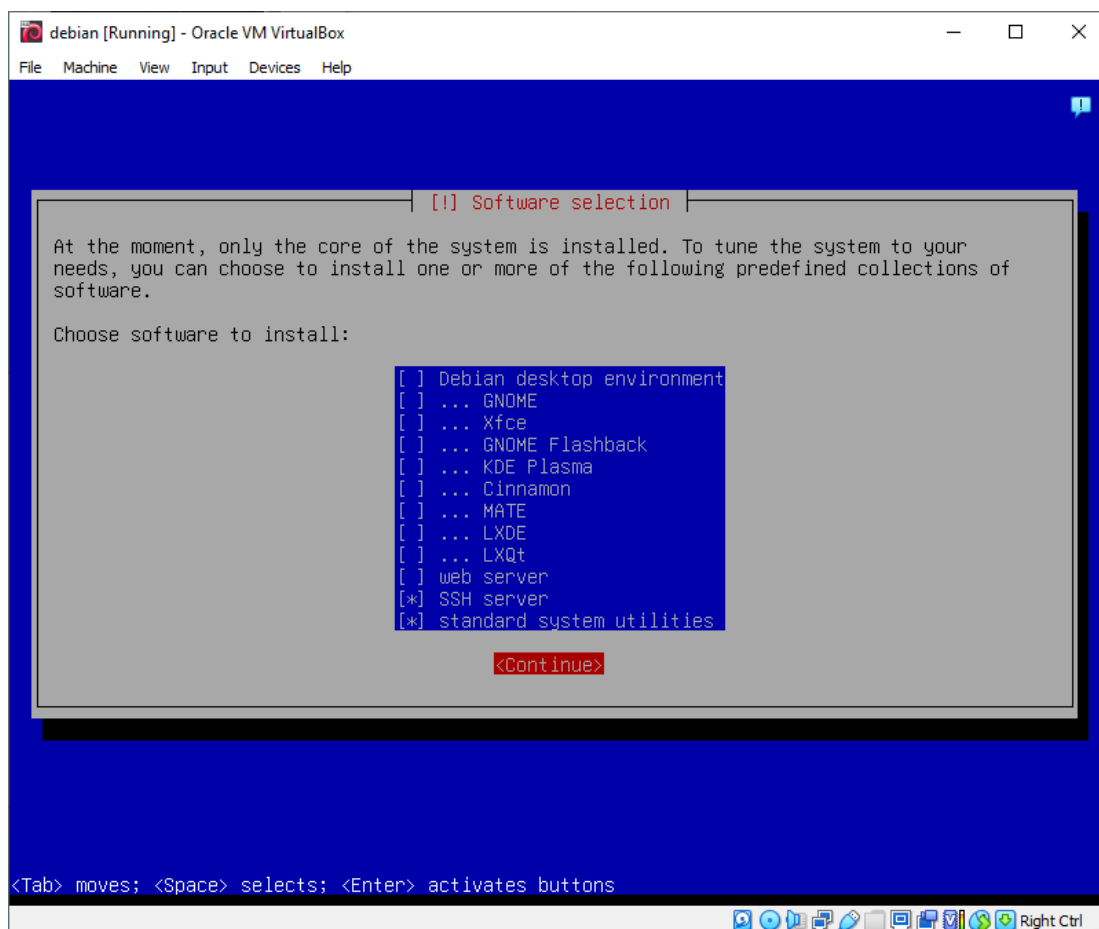
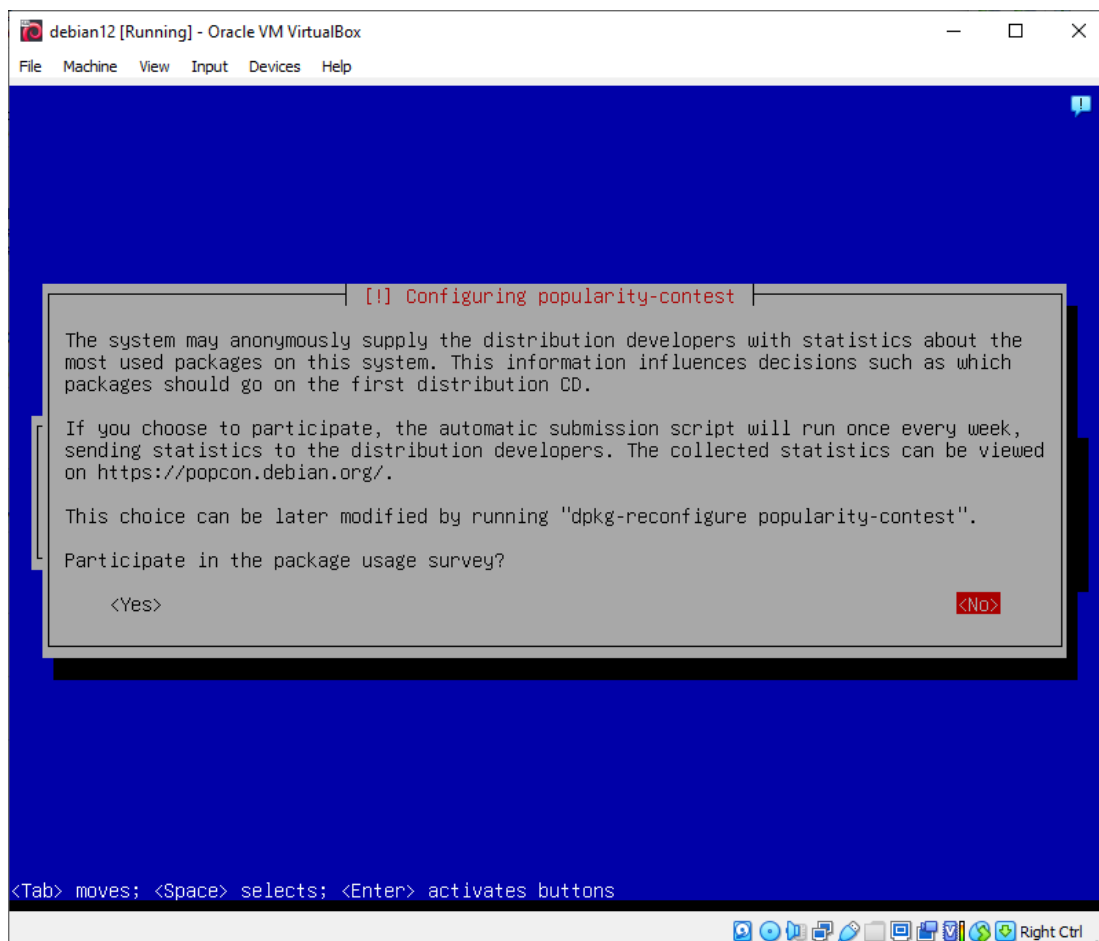




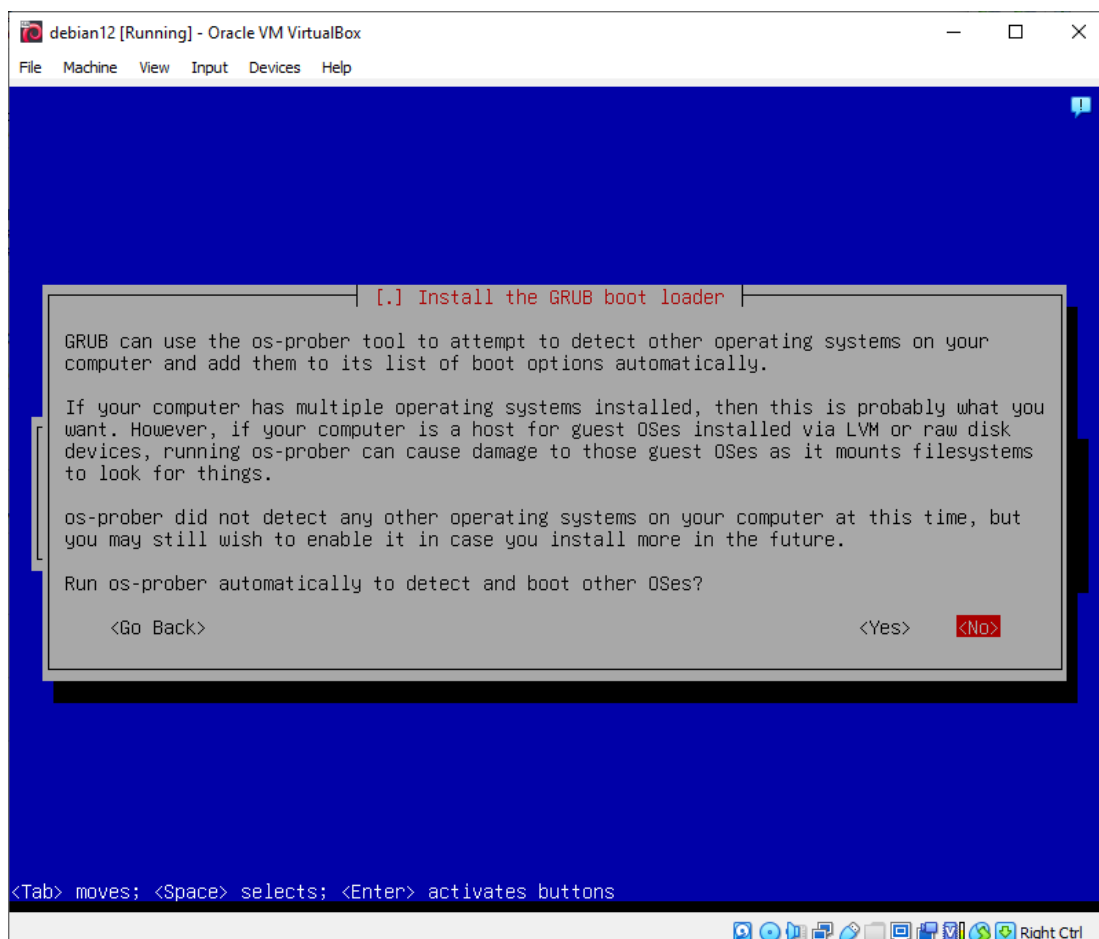
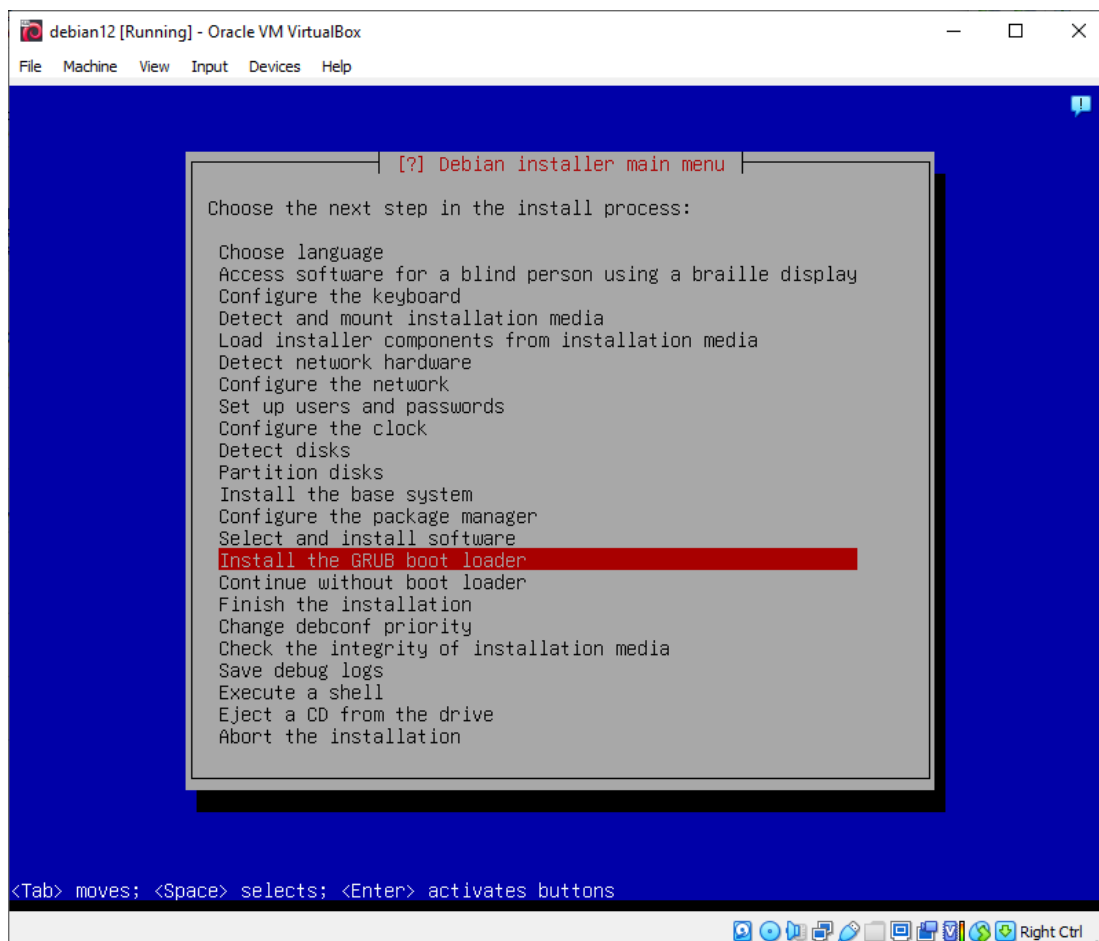


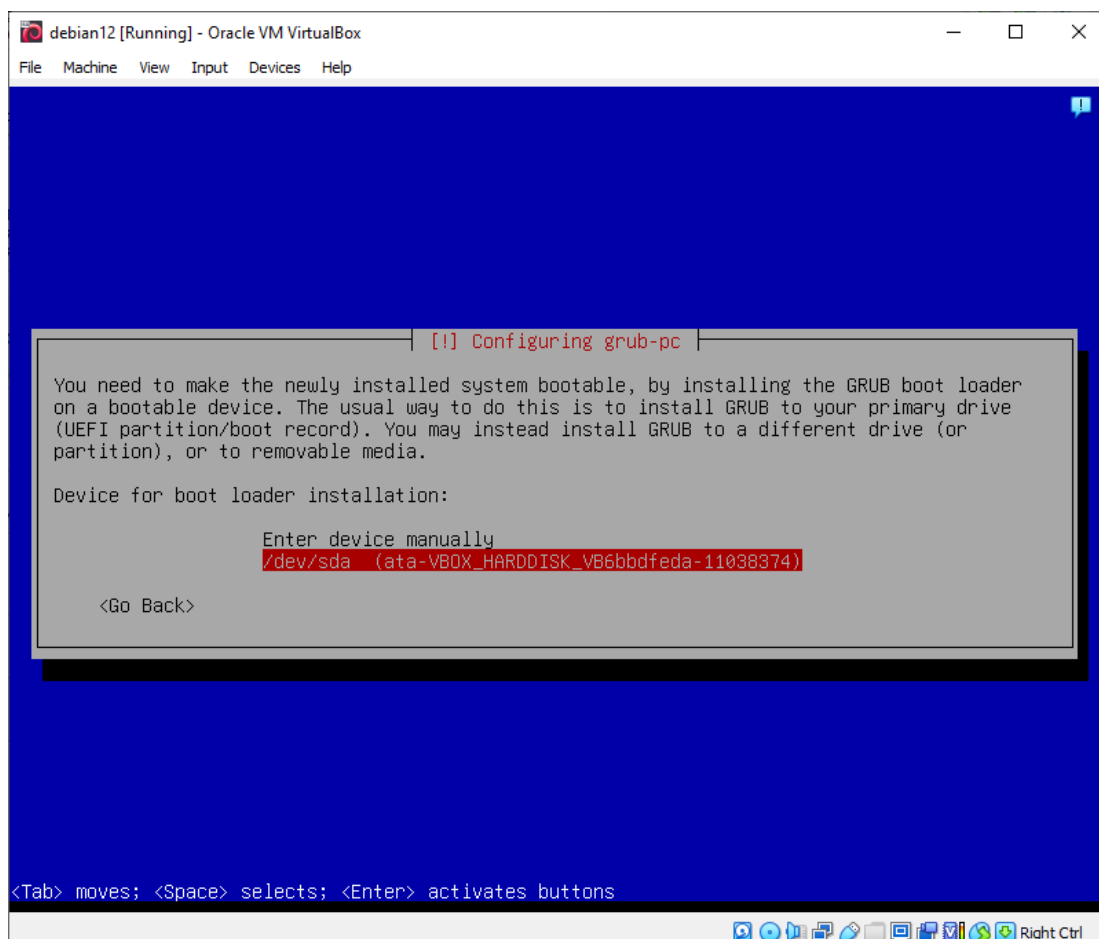
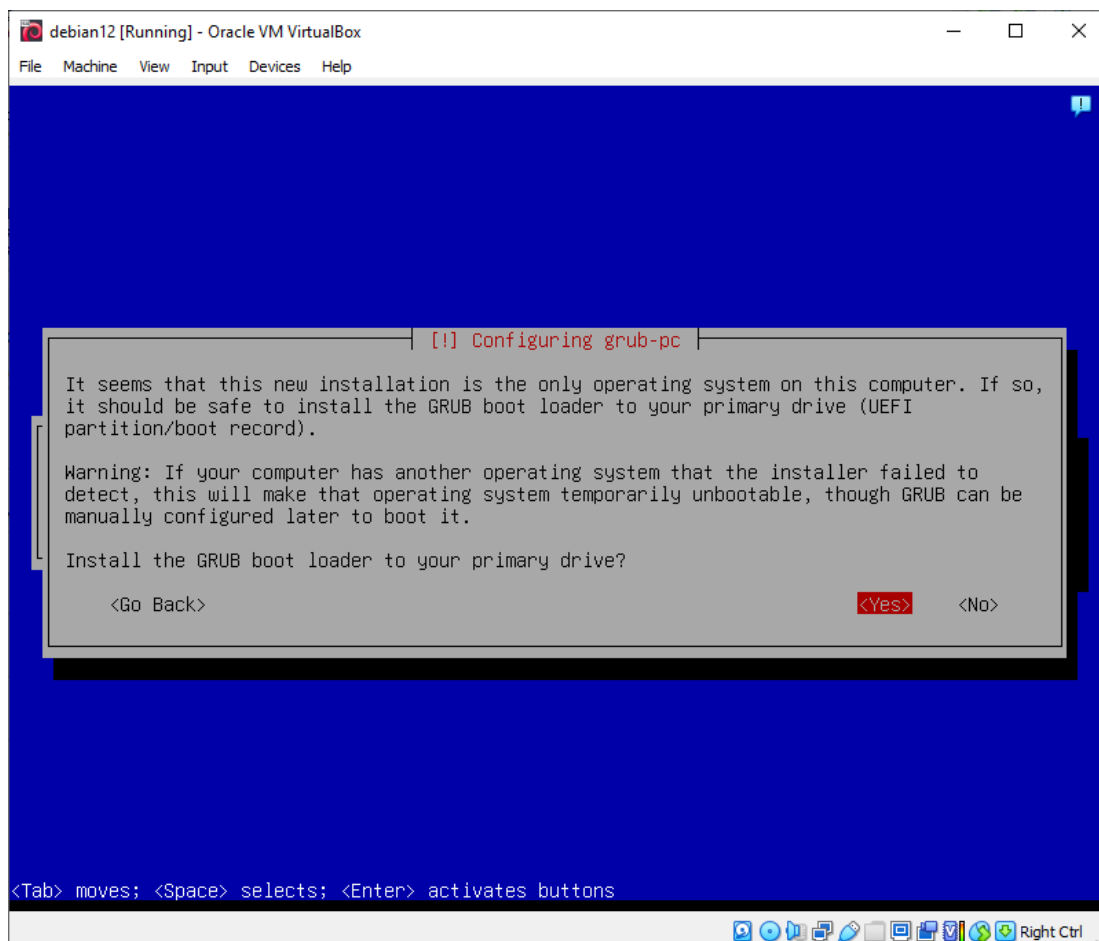


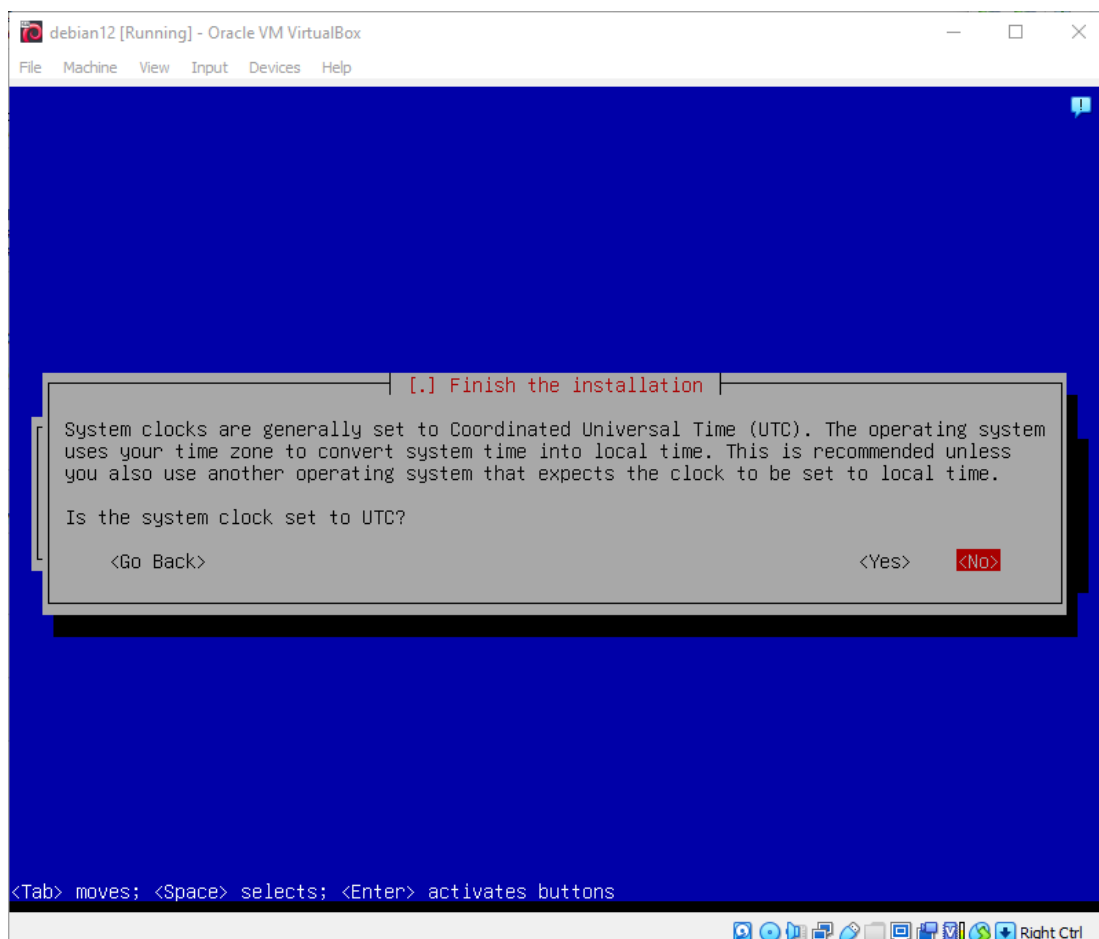
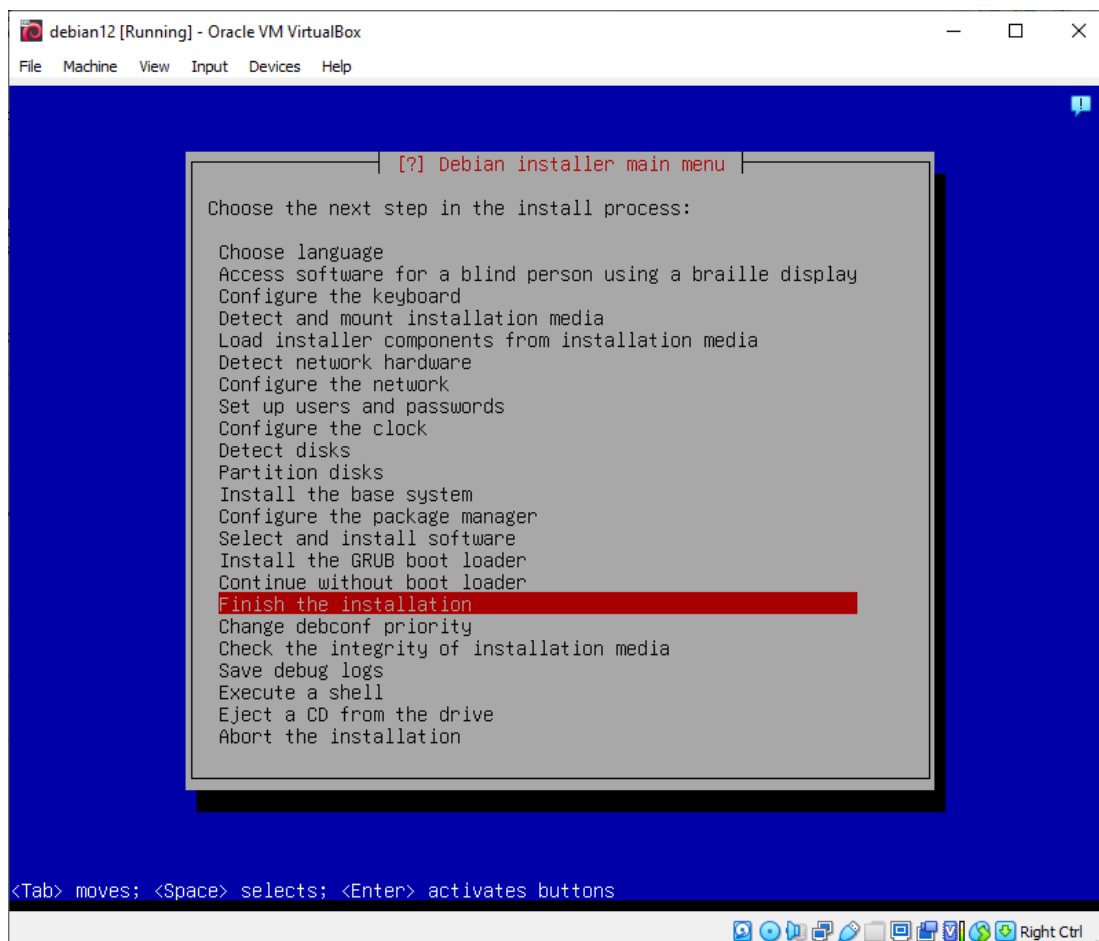




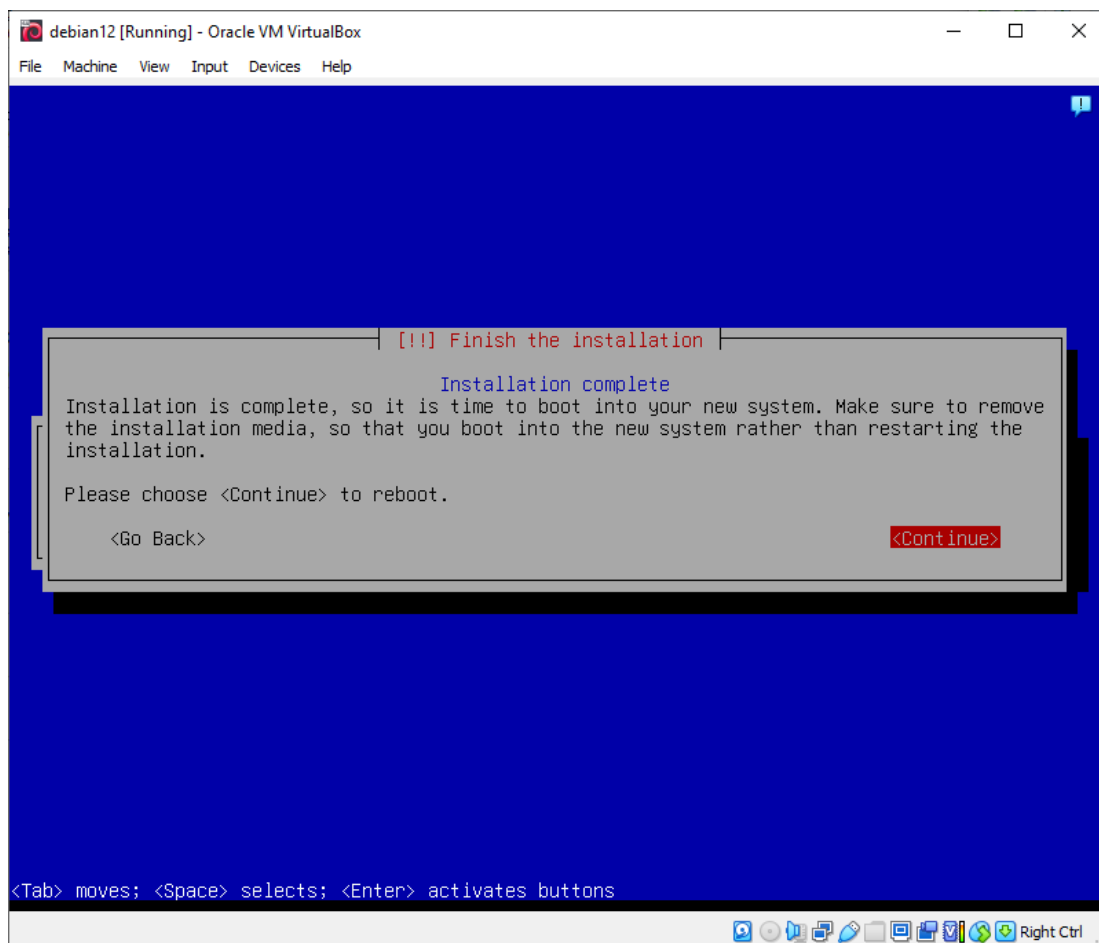




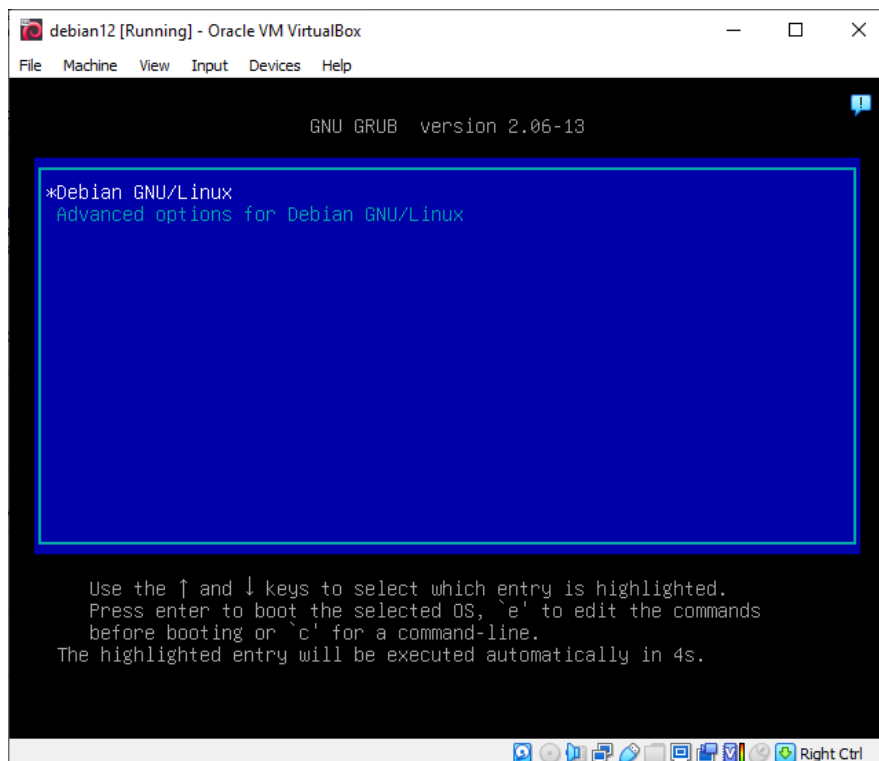




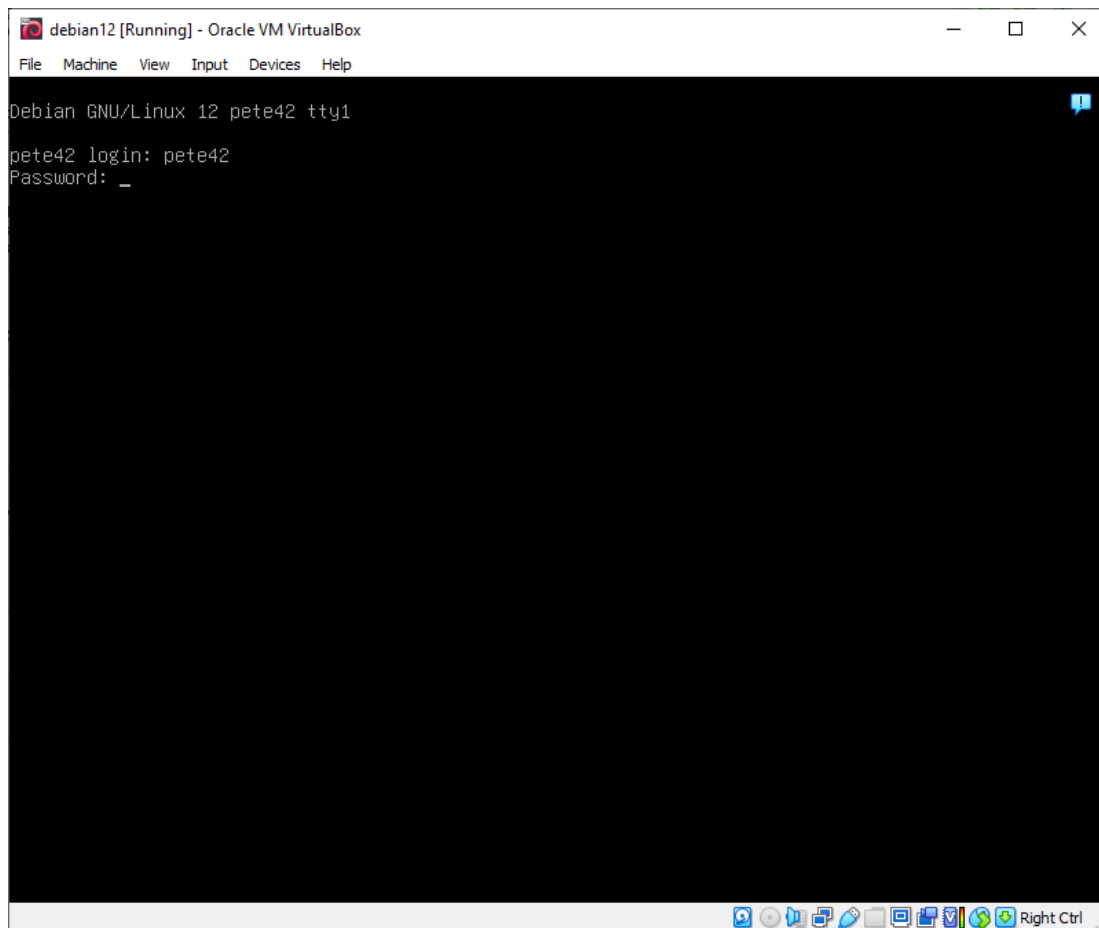
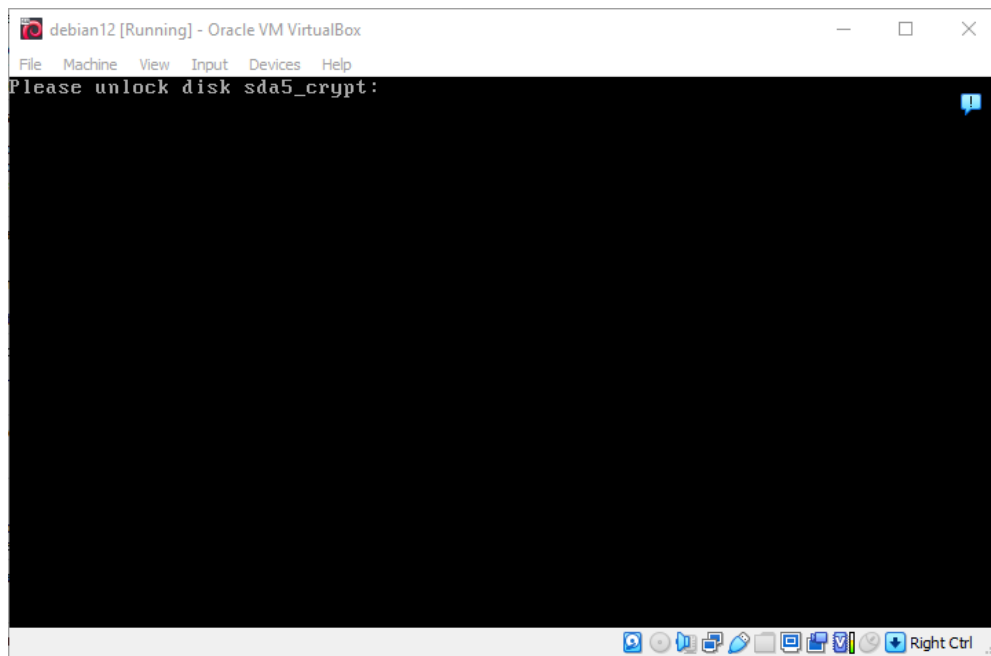
The ISO image is automatically unmounted



Reboot



Enter your passphrase when prompted e.g. A very complicated passphrase



After login

```
debian12 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Debian GNU/Linux 12 pete42 tty1

pete42 login: pete42
Password:
Linux pete42 6.1.0-13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.55-1 (2023-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
pete42@pete42:~$
```

Check disk partition layout

```
debian12 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Debian GNU/Linux 12 pete42 tty1

pete42 login: pete42
Password:
Linux pete42 6.1.0-13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.55-1 (2023-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
pete42@pete42:~$
pete42@pete42:~$
pete42@pete42:~$
pete42@pete42:~$ lsblk
NAME                                MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINTS
sda                                  8:0    0    8G  0 disk
├─sda1                              8:1    0 476M  0 part  /boot
├─sda2                              8:2    0    1K  0 part
├─sda5                              8:5    0   7.5G  0 part
│   └─sda5_crypt                    254:0    0   7.5G  0 crypt
│       ├─sda5_crypt-pet---vg--root 254:1    0   2.6G  0 lvm    /
│       ├─sda5_crypt-pet---vg--swap_1 254:2    0   952M  0 lvm    [SWAP]
│       └─sda5_crypt-pet---vg--home  254:3    0   3.7G  0 lvm    /home
sr0                                  11:0    1 1024M  0 rom
```

versus documented disk layout

```
wil@wil:~$ lsblk
NAME                                MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINT
sda                                  8:0    0   8G  0 disk
├─sda1                              8:1    0 487M  0 part  /boot
├─sda2                              8:2    0    1K  0 part
├─sda5                              8:5    0   7.5G  0 part
│   └─sda5_crypt                    254:0    0   7.5G  0 crypt
│       ├─wil--vg-root                254:1    0   2.8G  0 lvm    /
│       ├─wil--vg-swap_1              254:2    0   976M  0 lvm    [SWAP]
│       └─wil--vg-home                254:3    0   3.8G  0 lvm    /home
sr0                                  11:0    1 1024M  0 rom
```

Shutdown VM

Use command "sudo shutdown -h now" and enter your password to shutdown the VM

```
debian12 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Debian GNU/Linux 12 pete42 tty1

pete42 login: pete42
Password:
Linux pete42 6.1.0-13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.55-1 (2023-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
pete42@pete42:~$
pete42@pete42:~$
pete42@pete42:~$
pete42@pete42:~$ lsblk
NAME                                MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINTS
sda                                  8:0    0   8G  0 disk
├─sda1                              8:1    0 476M  0 part  /boot
├─sda2                              8:2    0    1K  0 part
├─sda5                              8:5    0   7.5G  0 part
│   └─sda5_crypt                    254:0    0   7.5G  0 crypt
│       ├─sda5_crypt-pet----vg--root 254:1    0   2.6G  0 lvm    /
│       ├─sda5_crypt-pet----vg--swap_1 254:2    0   952M  0 lvm    [SWAP]
│       └─sda5_crypt-pet----vg--home 254:3    0   3.7G  0 lvm    /home
sr0                                  11:0    1 1024M  0 rom
pete42@pete42:~$
pete42@pete42:~$
pete42@pete42:~$
pete42@pete42:~$
pete42@pete42:~$ sudo shutdown -h now
[sudo] password for pete42: _
```

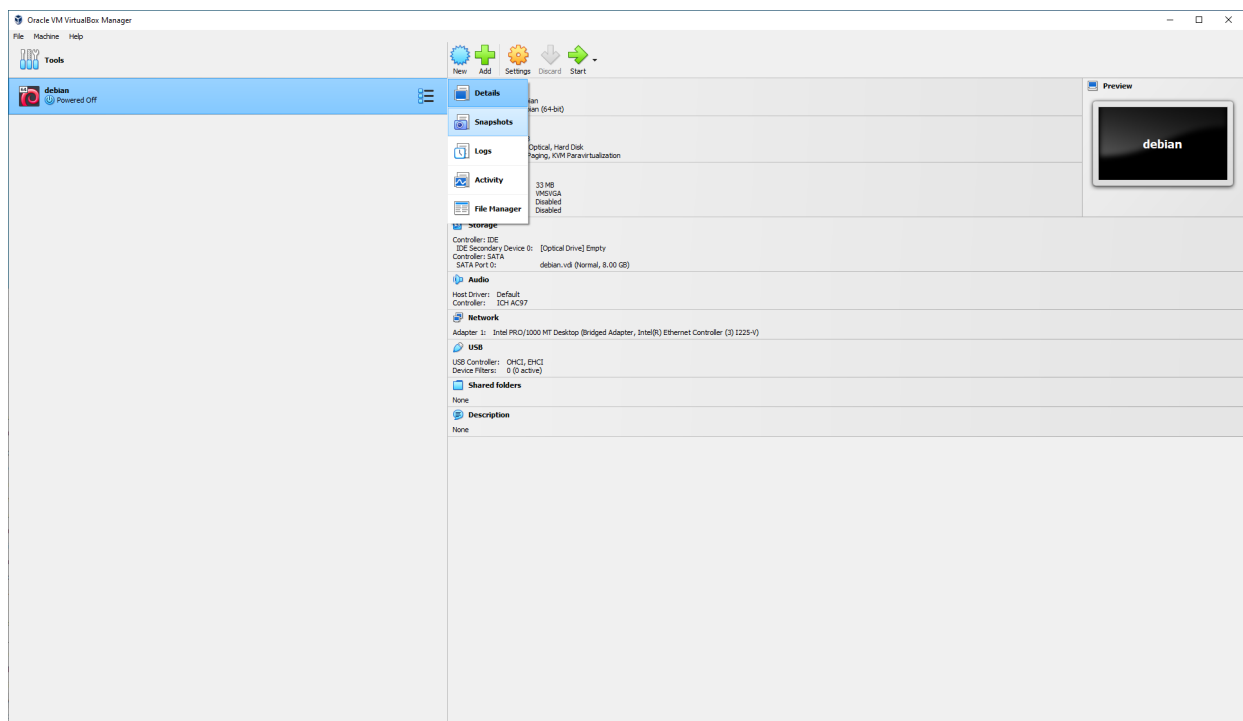
## Some (hopefully) useful information

This section has some hints and tips for setting up VirtualBox to be more useful as well as configuring the VM to meet the Born2beroot requirements.

### Snapshot the VM

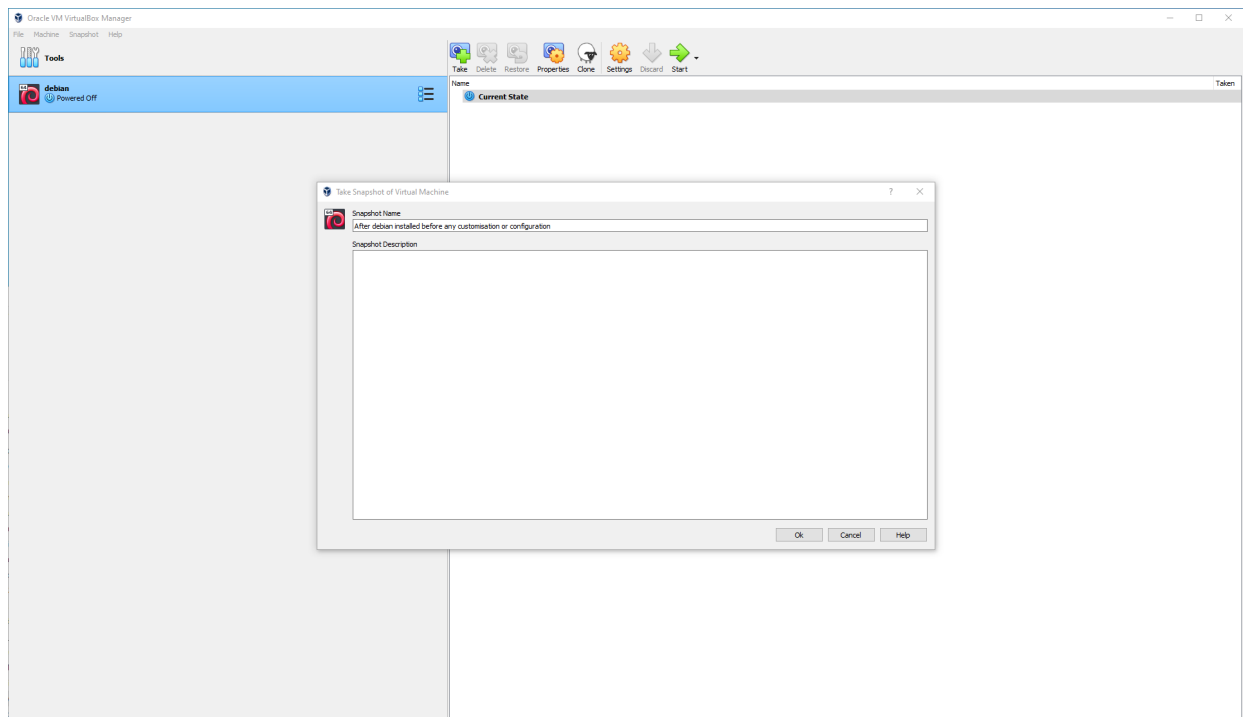
**IMPORTANT** before starting any customisation or configuration it is a very good idea to take a snapshot of the VM in it's current state which allows you to roll-back the VM to the status of the snapshot should things get screwed up because things have not gone to plan

Take a snapshot as shown below - it is best to do this when the VM is powered off as that ensures there is not activity that could result in data corruption!



Click the Take button in the menu bar and add details of what the snapshot contains - provide a reasonable amount of information as it is easy to forget what the status in when you have multiple snapshots and need to roll back to a specific status!!!!

Click OK to take the snapshot



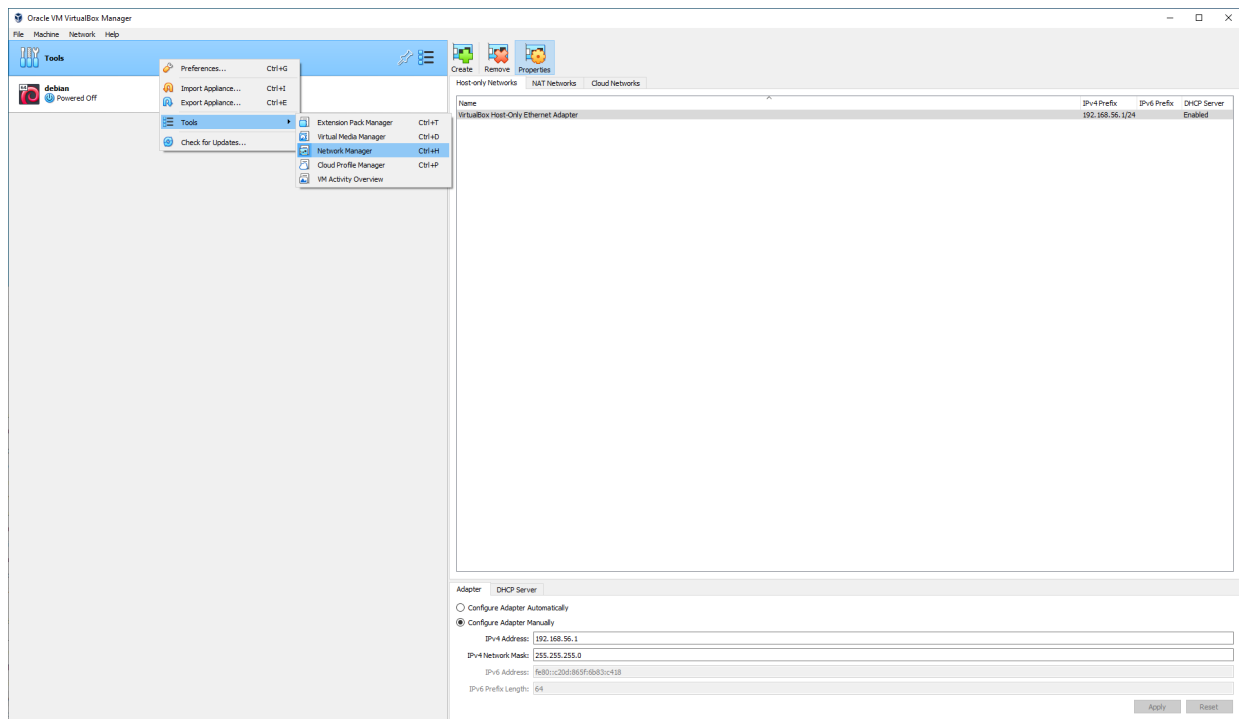
Remember to shutdown the VM and take a snapshot before you start doing anything dodgy or high risk - it will avoid a lot of grief.  
YOU HAVE BEEN WARNED

## Host-only Network

This is not required unless you need multiple VMs running in parallel to be able to communicate on thier own internal virtual network.

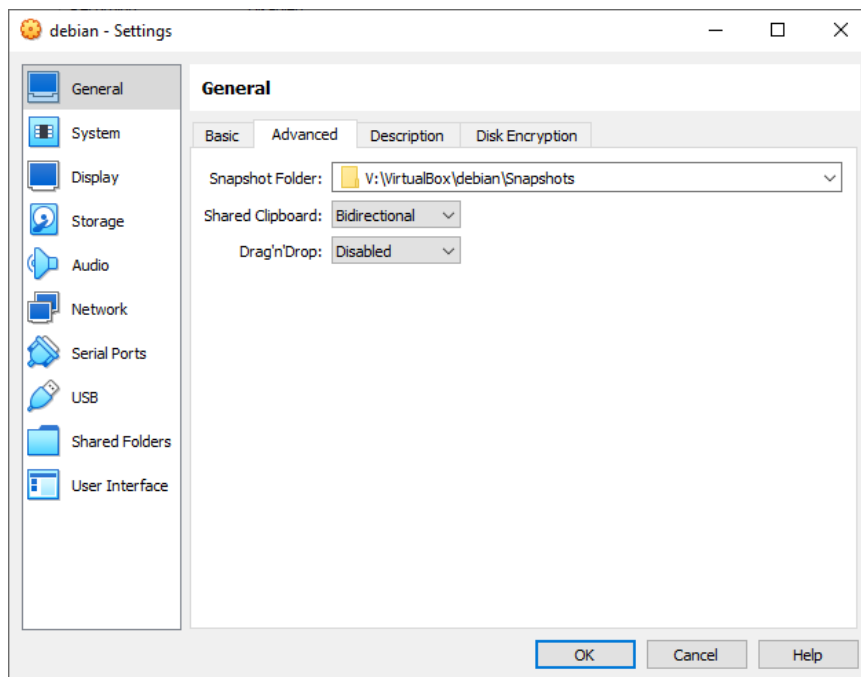
If a Host-Only network is required, right-click the Tools and view the Network Manager to access details of IP subnet etc. (as shown below)





## Shared Clipboard

Enable the shared clipboard to be able to copy/paste from the VM to the host desktop/laptop by clicking the Settings button (while the VM is selected on the left) and enabling the General-> Advanced - Shared Clipboard option



## Debian vs Rocky

Choice of debian over Rocky linux because documentation recommended it for "beginners" - Rocky is a derivative of Red Hat and is more common in enterprise use as it is owned by IBM. Debian is a community supported Linux distribution with a wide variety of use from typical office functions and email through to games and networking.

## SELinux vs AppArmor

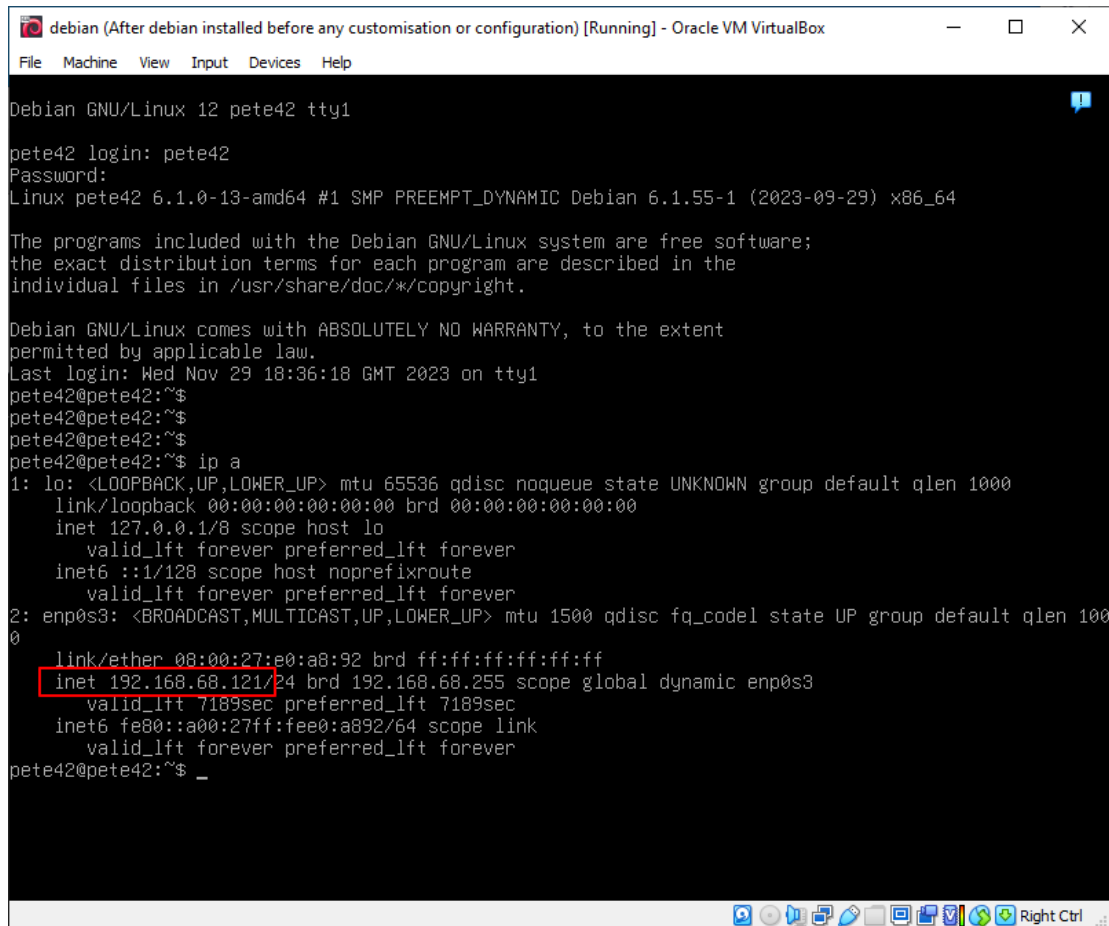
SELinux is the Rocky/Red Hat/Fedora and others for additional security configurations whilst AppArmor is used by debian/ubuntu/and others for the same purpose. This article provides a good description and comparison of each <https://www.techtarget.com/searchdatacenter/tip/Compare-two-Linux-security-modules-SELinux-vs-AppArmor#:~:text=It's%20important%20to%20understand%20that,Ubuntu%20Derivatives%20use%20AppArmor>.

## Terminal access

VirtualBox has it's own terminal that pops up when the VM is started. Whilst it is functional a much better terminal is available that support SSH and copy/paste etc. between host desktop/laptop and the VM. You can download a version of MobaXterm Home edition from from here <https://mobaxterm.mobatek.net/download-home-edition.html>

After installing that you can access the VM using MobaXterm following the steps below

Find the IP address assigned to the VM from the VirtualBox terminal window with the command: `ip a`  
(a for address) - the IP address is outlined in red below



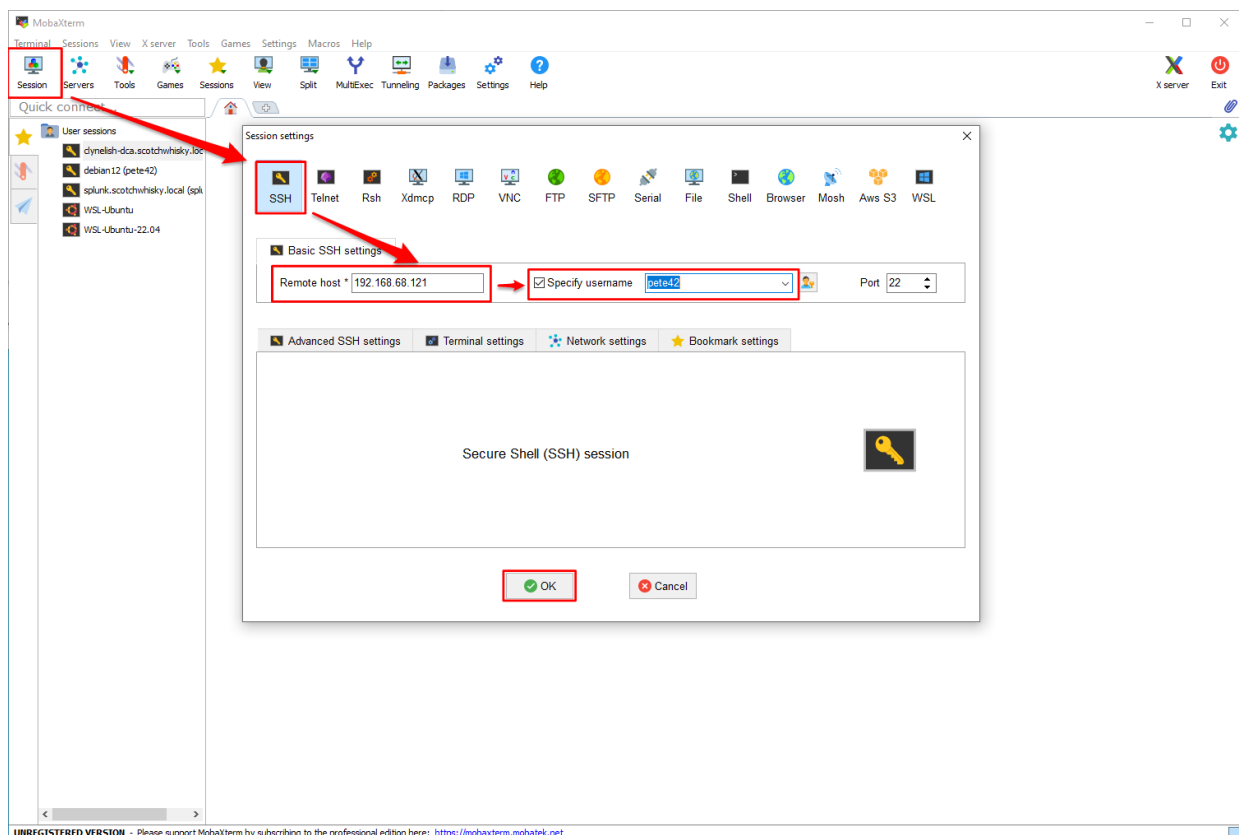
```
Debian GNU/Linux 12 pete42 tty1

pete42 login: pete42
Password:
Linux pete42 6.1.0-13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.55-1 (2023-09-29) x86_64

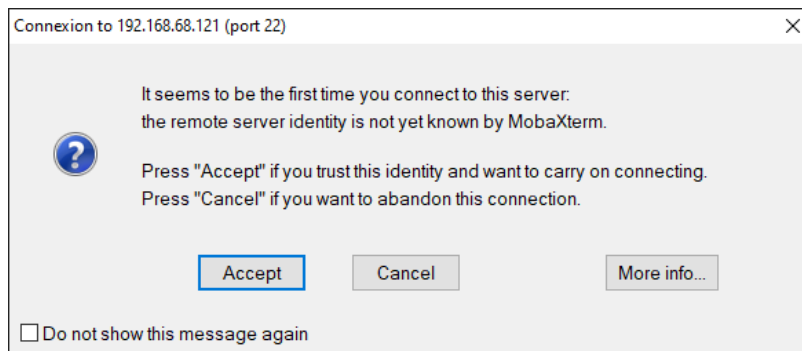
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Nov 29 18:36:18 GMT 2023 on tty1
pete42@pete42:~$
pete42@pete42:~$
pete42@pete42:~$
pete42@pete42:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e0:a8:92 brd ff:ff:ff:ff:ff:ff
    inet 192.168.68.121/24 brd 192.168.68.255 scope global dynamic enp0s3
        valid_lft 7189sec preferred_lft 7189sec
    inet6 fe80::a00:27ff:fee0:a892/64 scope link
        valid_lft forever preferred_lft forever
pete42@pete42:~$ _
```

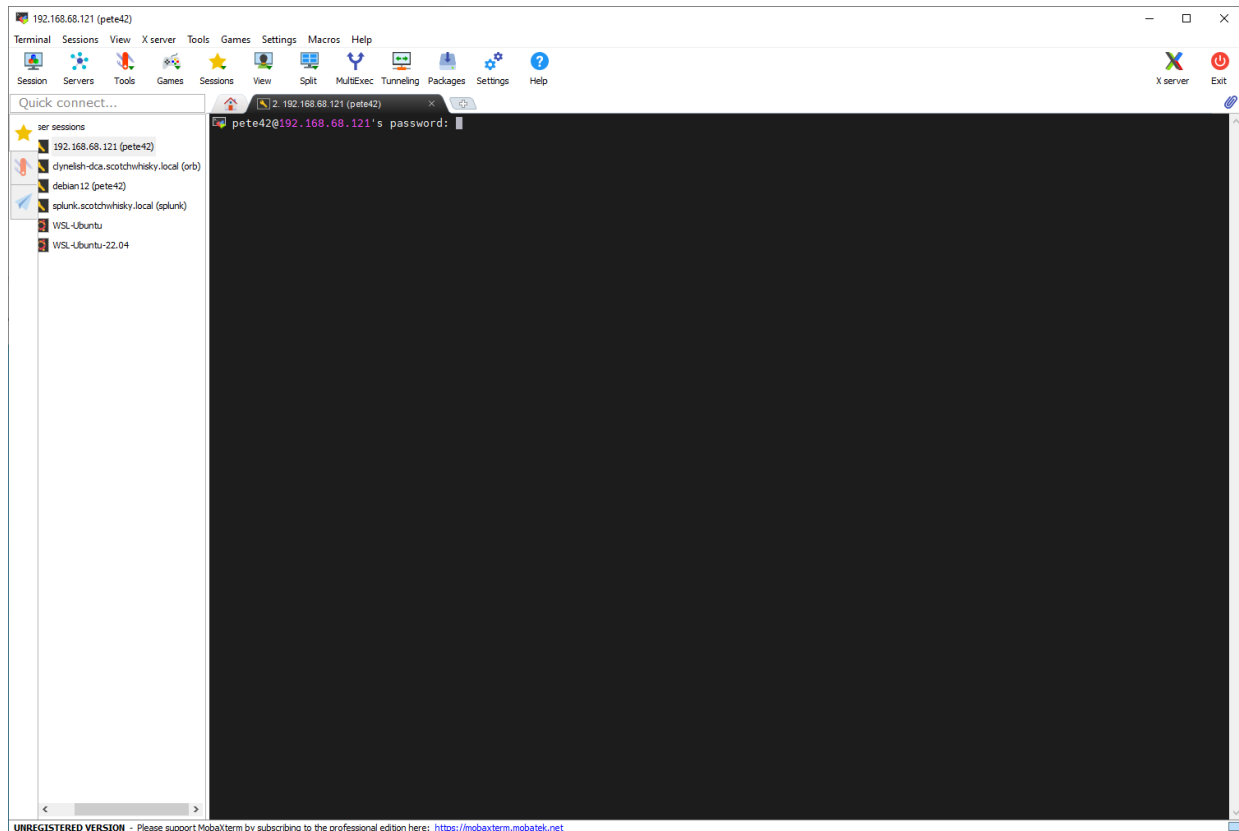
Start the MobaXterm program and start a new session as shown below



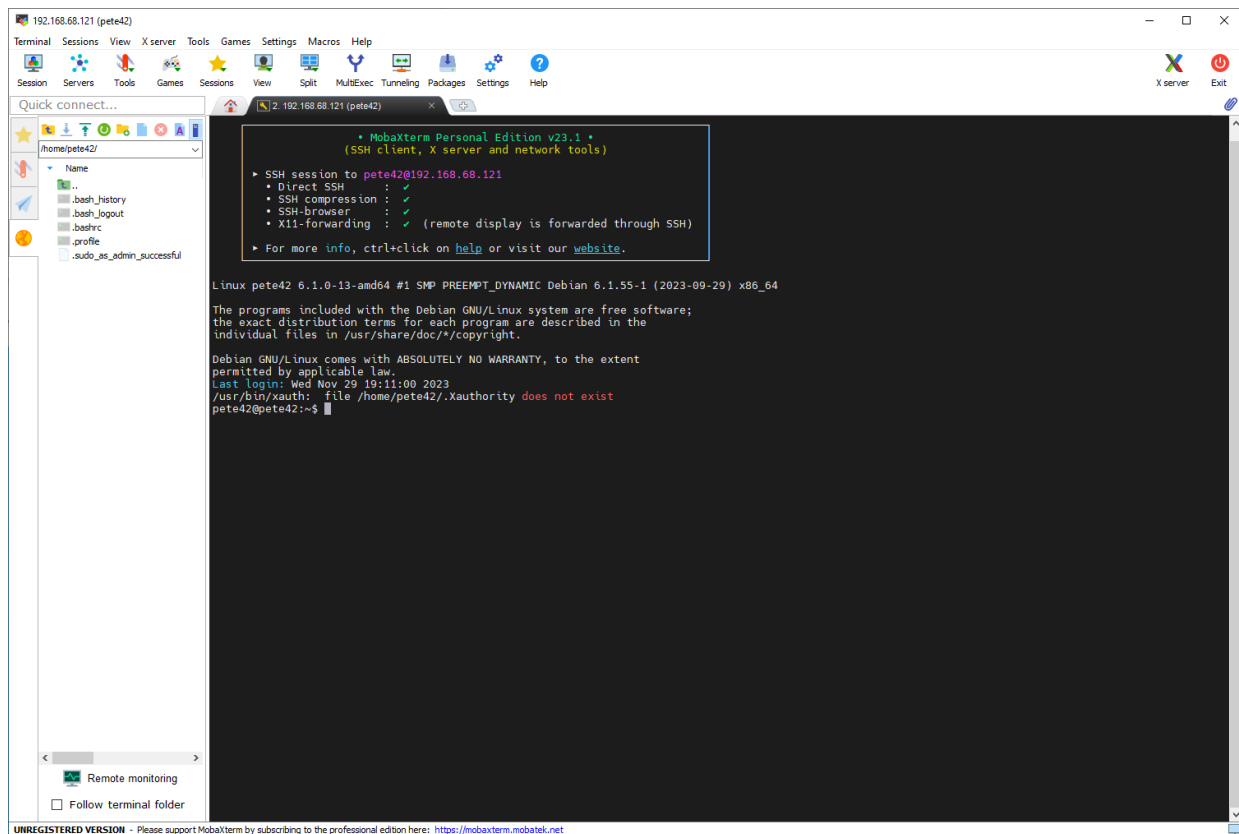
The first time you connect to a new system using SSH it prompts you to save the signature of the system - click Accept



Next enter your password



You will be asked if you want to save the password - your choice and then you will be logged into the VM



Now that MobaXterm is used to access the VM the remaining instructions will include the commands used as text instead of the screenshots used previously.

Note the message below is normal as there is no graphical (X11) software installed - this is a requirement of Born2beroot

```
/usr/bin/xauth: file /home/pete42/.Xauthority does not exist
```

## Install Firewall

Debian Uncomplicated FireWall (ufw) setup - more detail here <https://www.cyberciti.biz/faq/set-up-a-firewall-with-ufw-on-debian-12-linux/>

Use sudo to install the firewall software as shown below

First check for any updates

```
pete42@pete42:~$ sudo apt update
[sudo] password for pete42:
Hit:1 http://security.debian.org/debian-security bookworm-security InRelease
Hit:2 https://deb.debian.org/debian bookworm InRelease
Hit:3 https://deb.debian.org/debian bookworm-updates InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
pete42@pete42:~$
```

Install ufw

```
pete42@pete42:~$ sudo apt install ufw
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  iptables libip6tc2 libnetfilter-conntrack3 libnfnctlink0
Suggested packages:
  firewallld rsyslog
The following NEW packages will be installed:
  iptables libip6tc2 libnetfilter-conntrack3 libnfnctlink0 ufw
0 upgraded, 5 newly installed, 0 to remove and 0 not upgraded.
Need to get 603 kB of archives.
After this operation, 3,606 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 https://deb.debian.org/debian bookworm/main amd64 libip6tc2 amd64 1.8.9-2 [19.4 kB]
Get:2 https://deb.debian.org/debian bookworm/main amd64 libnfnctlink0 amd64 1.0.2-2 [15.1 kB]
Get:3 https://deb.debian.org/debian bookworm/main amd64 libnetfilter-conntrack3 amd64 1.0.9-3 [40.7 kB]
Get:4 https://deb.debian.org/debian bookworm/main amd64 iptables amd64 1.8.9-2 [360 kB]
Get:5 https://deb.debian.org/debian bookworm/main amd64 ufw all 0.36.2-1 [168 kB]
Fetched 603 kB in 0s (6,460 kB/s)
Preconfiguring packages ...
```

```

Selecting previously unselected package libip6tc2:amd64.
(Reading database ... 29028 files and directories currently installed.)
Preparing to unpack .../libip6tc2_1.8.9-2_amd64.deb ...
Unpacking libip6tc2:amd64 (1.8.9-2) ...
Selecting previously unselected package libnftnl0:amd64.
Preparing to unpack .../libnftnl0_1.0.2-2_amd64.deb ...
Unpacking libnftnl0:amd64 (1.0.2-2) ...
Selecting previously unselected package libnetfilter-contrack3:amd64.
Preparing to unpack .../libnetfilter-contrack3_1.0.9-3_amd64.deb ...
Unpacking libnetfilter-contrack3:amd64 (1.0.9-3) ...
Selecting previously unselected package iptables.
Preparing to unpack .../iptables_1.8.9-2_amd64.deb ...
Unpacking iptables (1.8.9-2) ...
Selecting previously unselected package ufw.
Preparing to unpack .../archives/ufw_0.36.2-1_all.deb ...
Unpacking ufw (0.36.2-1) ...
Setting up libip6tc2:amd64 (1.8.9-2) ...
Setting up libnftnl0:amd64 (1.0.2-2) ...
Setting up libnetfilter-contrack3:amd64 (1.0.9-3) ...
Setting up iptables (1.8.9-2) ...
update-alternatives: using /usr/sbin/iptables-legacy to provide /usr/sbin/iptables (iptables) in auto mode
update-alternatives: using /usr/sbin/ip6tables-legacy to provide /usr/sbin/ip6tables (ip6tables) in auto mode
update-alternatives: using /usr/sbin/iptables-nft to provide /usr/sbin/iptables (iptables) in auto mode
update-alternatives: using /usr/sbin/ip6tables-nft to provide /usr/sbin/ip6tables (ip6tables) in auto mode
update-alternatives: using /usr/sbin/arptables-nft to provide /usr/sbin/arptables (arptables) in auto mode
update-alternatives: using /usr/sbin/eptables-nft to provide /usr/sbin/eptables (eptables) in auto mode
Setting up ufw (0.36.2-1) ...

Creating config file /etc/ufw/before.rules with new version

Creating config file /etc/ufw/before6.rules with new version

Creating config file /etc/ufw/after.rules with new version

Creating config file /etc/ufw/after6.rules with new version
Created symlink /etc/systemd/system/multi-user.target.wants/ufw.service → /lib/systemd/system/ufw.service.
Processing triggers for libc-bin (2.36-9+deb12u3) ...
Processing triggers for man-db (2.11.2-2) ...
pete42@pete42:~$

```

#### configure fw

```

pete42@pete42:~$ sudo ufw status
Status: inactive
pete42@pete42:~$
pete42@pete42:~$
pete42@pete42:~$
pete42@pete42:~$ sudo ufw allow 22/tcp      ## SSH default port
Rules updated
Rules updated (v6)
pete42@pete42:~$
pete42@pete42:~$
pete42@pete42:~$ sudo ufw enable           ## enable fw
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
pete42@pete42:~$
pete42@pete42:~$
pete42@pete42:~$ sudo ufw reload           ## reload fw
Firewall reloaded
pete42@pete42:~$
pete42@pete42:~$
pete42@pete42:~$ sudo ufw status verbose  ## fw status
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To Action From
--
22/tcp ALLOW IN Anywhere
22/tcp (v6) ALLOW IN Anywhere (v6)

pete42@pete42:~$

```

Test you can still connect by entering CTRL+d (logoff) to disconnect from the terminal session in MobaXterm then type "r" to restart the session

Now open port 4242 for SSSH as required by the Born2beroot

```

pete42@pete42:~$ sudo ufw allow 4242/tcp    ## SSH required port
Rule added
Rules added (v6)
pete42@pete42:~$ sudo ufw reload           ## reload fw
Firewall reloaded
pete42@pete42:~$ sudo ufw status verbose  ## fw status
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To Action From
--

```

22/tcp	ALLOW	IN	Anywhere
4242/tcp	ALLOW	IN	Anywhere
22/tcp (v6)	ALLOW	IN	Anywhere (v6)
4242/tcp (v6)	ALLOW	IN	Anywhere (v6)

```
pete42@pete42:~$
```

## Hostname

Hostname of the VM must be set to login name ending in 42 e.g. pete42.  
This was set at install time so doesn't need changing.

Born2beroot documentation says you will need to change the hostname during your evaluation.

Use the command

```
pete42@pete42:~$ sudo hostnamectl hostname                ## display current hostname
pete42
pete42@pete42:~$ sudo hostnamectl hostname andrew42       ## change hostname to andrew42
pete42@pete42:~$ sudo hostnamectl hostname                ## display current hostname
sudo: unable to resolve host andrew42: Name or service not known
andrew42
pete42@pete42:~$ sudo hostnamectl hostname pete42         ## change hostname back to pete42
sudo: unable to resolve host andrew42: Name or service not known
pete42@pete42:~$ sudo hostnamectl hostname                ## display current hostname
pete42
pete42@pete42:~$ ping pete42                             ## display current hostname
PING pete42.scotchwhisky.local (127.0.1.1) 56(84) bytes of data.
64 bytes from pete42.scotchwhisky.local (127.0.1.1): icmp_seq=1 ttl=64 time=0.026 ms
64 bytes from pete42.scotchwhisky.local (127.0.1.1): icmp_seq=2 ttl=64 time=0.104 ms
^C                                                         ## CTRL+c to interrupt command
--- pete42.scotchwhisky.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1024ms
rtt min/avg/max/mdev = 0.026/0.065/0.104/0.039 ms
pete42@pete42:~$
```

## SSH (Secure SHell)

SSH (Secure SHell) is used to access most Linux/UNIX systems as it uses an encrypted connection between the client and target system. Default port for SSH is port 22. It needs to be configured for port 4242 to meet requirements.

/etc/ssh/sshd\_config contains the SSH daemon configuration - make sure you edit sshd\_config and not ssh\_config

Change the line

#Port 22

to

Port 4242

and save the changes.

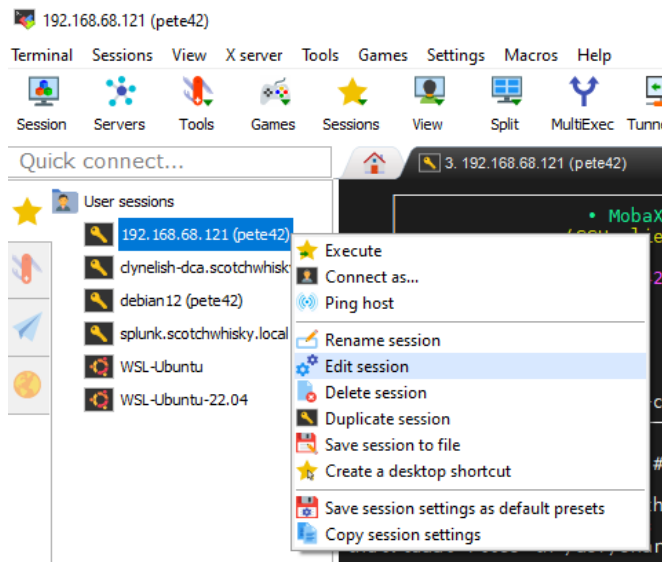
Restart the SSH daemon to make the change effective

```
pete42@pete42:~$ sudo systemctl restart sshd
pete42@pete42:~$ sudo systemctl status sshd
• ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
   Active: active (running) since Thu 2023-11-30 15:47:30 GMT; 10s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 1453 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
  Main PID: 1454 (sshd)
    Tasks: 1 (limit: 2338)
   Memory: 1.4M
      CPU: 9ms
   CGroup: /system.slice/ssh.service
           └─1454 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Nov 30 15:47:30 pete42 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Nov 30 15:47:30 pete42 sshd[1454]: Server listening on 0.0.0.0 port 4242.
Nov 30 15:47:30 pete42 sshd[1454]: Server listening on :: port 4242.
Nov 30 15:47:30 pete42 systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
pete42@pete42:~$
```

Close your MobaXterm session and restart it

The restart doesn't work because the SSH daemon is now listening on port 4242 - edit the MobaXterm session settings and change the port 22 to 4242 and then try again to connect



Now remove the port 22 rule from the firewall so that nothing can connect on port 22

```
pete42@pete42:~$ sudo ufw status numbered
Status: active

    To      Action      From
    --      -
[ 1] 22/tcp    ALLOW IN    Anywhere
[ 2] 4242/tcp   ALLOW IN    Anywhere
[ 3] 22/tcp (v6) ALLOW IN    Anywhere (v6)
[ 4] 4242/tcp (v6) ALLOW IN    Anywhere (v6)

pete42@pete42:~$ sudo ufw delete 1
Deleting:
allow 22/tcp
Proceed with operation (y|n)? y
Rule deleted
pete42@pete42:~$ sudo ufw status numbered
Status: active

    To      Action      From
    --      -
[ 1] 4242/tcp   ALLOW IN    Anywhere
[ 2] 22/tcp (v6) ALLOW IN    Anywhere (v6)
[ 3] 4242/tcp (v6) ALLOW IN    Anywhere (v6)

pete42@pete42:~$ sudo ufw delete 2
Deleting:
allow 22/tcp
Proceed with operation (y|n)? y
Rule deleted (v6)
pete42@pete42:~$ sudo ufw reload      ## reload fw
Firewall reloaded
pete42@pete42:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

    To      Action      From
    --      -
4242/tcp    ALLOW IN    Anywhere
4242/tcp (v6) ALLOW IN    Anywhere (v6)

pete42@pete42:~$
```

Now SSH can only be accessed over port 4242

## sudo configuration

sudo (switch **user** and **do**) allows a user to execute privileged commands i.e. as if they were the root user

You are prompted for your own user password the first time you use the sudo command and thereafter you will not be prompted on every sudo command (depends upon session timeouts etc.)

sudo is controlled by the file /etc/sudoers - it should not be edited directly, but instead should use the visudo command (which uses the nano editor to edit the file and it is syntax checked before being updated)

Other Linux flavours use the vi editor hence the name for the command visudo

As I don't know how to use nano and I prefer vi/vim you can change the edit as follows

```
pete42@pete42:~$ sudo update-alternatives --config editor
There are 2 choices for the alternative editor (providing /usr/bin/editor).
```

Selection	Path	Priority	Status
* 0	/bin/nano	40	auto mode
1	/bin/nano	40	manual mode
2	/usr/bin/vim.tiny	15	manual mode

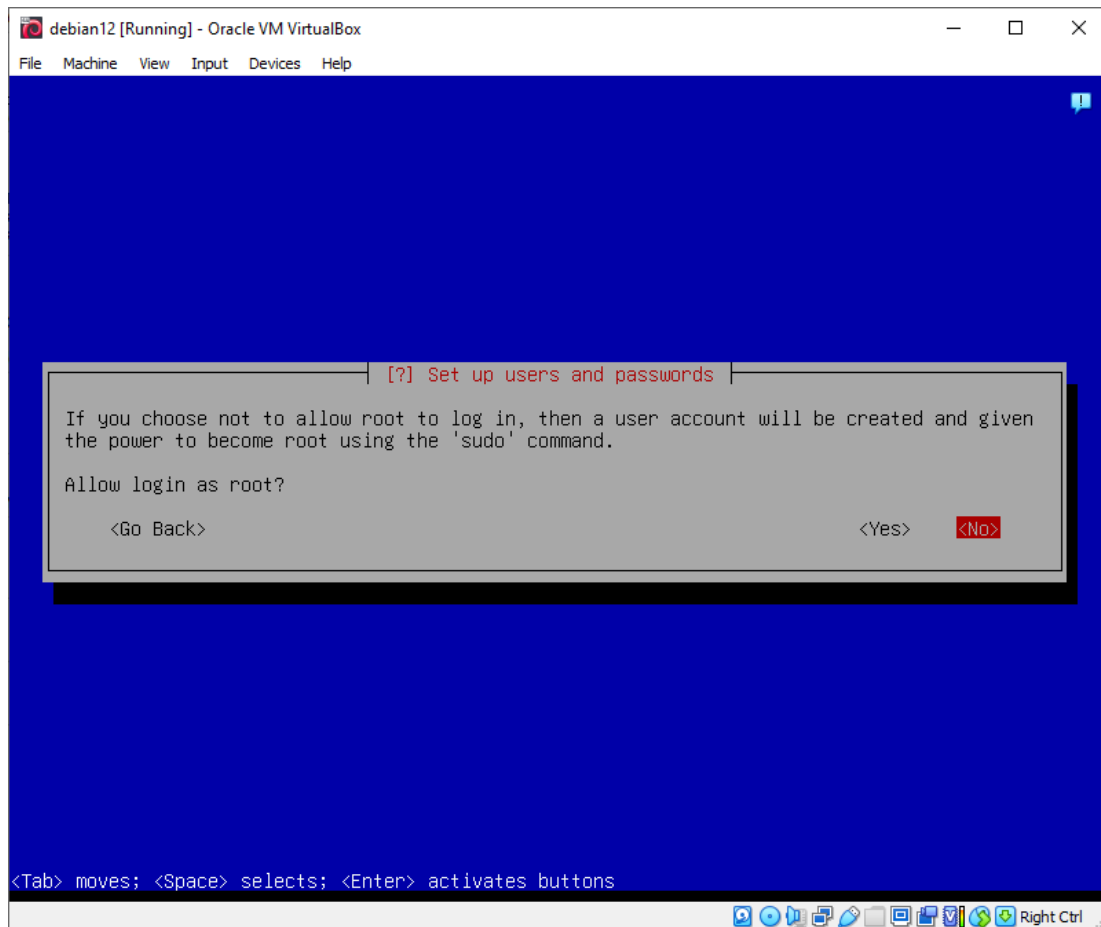
Press <enter> to keep the current choice[\*], or type selection number: 2  
 update-alternatives: using /usr/bin/vim.tiny to provide /usr/bin/editor (editor) in manual mode  
 pete42@pete42:~\$

The visudo command will now use the vi/vim editor from now on 😊

Use the visudo command to edit the sudoers file - upon doing so we can see the following lines

```
# Allow members of group sudo to execute any command
%sudo  ALL=(ALL:ALL) ALL
```

This allows all members of the sudo group to execute privileged commands and was configured automatically because the option to not allow root user login was selected at installation time (as shown below)



????????? Need to add sudo configuration steps here ??????????

The same configuration option caused my user (pete42) to be added to the sudo group which can be verified as follows

```
pete42@pete42:~$ id
uid=1000(pete42) gid=1000(pete42)
groups=1000(pete42),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),100(users),106(netdev)
pete42@pete42:~$
```

### Add user to group

Born2beroot requires that your user (pete42) is a member of both the sudo group (as seen above) and the group **user42**

The list of groups that user pete42 belongs to does not include the user42 group so it needs to be created and the user pete42 added to it.

```
pete42@pete42:~$ sudo grep user42 /etc/group      ## check if group user42 exists
pete42@pete42:~$
pete42@pete42:~$ sudo cat /etc/group             ## list groups that exist
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
```



```
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:pete42
floppy:x:25:pete42
tape:x:26:
sudo:x:27:pete42
audio:x:29:pete42
dip:x:30:pete42
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
shadow:x:42:
utmp:x:43:
video:x:44:pete42
sasl:x:45:
plugdev:x:46:pete42
staff:x:50:
games:x:60:
users:x:100:pete42
nogroup:x:65534:
systemd-journal:x:999:
systemd-network:x:998:
crontab:x:101:
input:x:102:
sgx:x:103:
kvm:x:104:
render:x:105:
netdev:x:106:pete42
messagebus:x:107:
systemd-timesync:x:997:
ssh:x:108:
pete42:x:1000:
pete42@pete42:~$
```

Create the user42 group

```
pete42@pete42:~$ sudo groupadd user42
pete42@pete42:~$ sudo grep user42 /etc/group      ## check if group user42 exists
user42:x:1001:
pete42@pete42:~$
```

Add the user (pete42) to the group user42

```
pete42@pete42:~$ id                                ## list current groups
uid=1000(pete42) gid=1000(pete42)
groups=1000(pete42),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),100(users),106(netdev)
pete42@pete42:~$ sudo usermod -a -G user42 pete42    ## add user to group
pete42@pete42:~$ id                                ## list groups but not present - need to login again!
uid=1000(pete42) gid=1000(pete42)
groups=1000(pete42),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),100(users),106(netdev)
pete42@pete42:~$ su - pete42                        ## login user pete42 again
Password:
pete42@pete42:~$ id                                ## now group user42 is present :-)
uid=1000(pete42) gid=1000(pete42)
groups=1000(pete42),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),100(users),106(netdev),1001(user42)
pete42@pete42:~$
logout
pete42@pete42:~$
```

Create a new user and add to a group

Born2beroot requires during evaluation the creation of a new user and add the user to a group

???????????????????????????????? TO BE COMPLETED ??????????????????????

## Password policy

This would be a good time to take a snapshot backup in case you screw up the password complexity rules and get locked out!!!!!!

Set password policy rules - see here for more details [https://www.server-world.info/en/note?os=Debian\\_12&p=pam&f=1](https://www.server-world.info/en/note?os=Debian_12&p=pam&f=1)

Install password quality check library

```
pete42@pete42:~$ sudo apt install libpam-pwquality
```

```
[sudo] password for pete42:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  cracklib-runtime libcrack2 libpwquality-common libpwquality1
The following NEW packages will be installed:
  cracklib-runtime libcrack2 libpam-pwquality libpwquality-common libpwquality1
0 upgraded, 5 newly installed, 0 to remove and 0 not upgraded.
Need to get 264 kB of archives.
After this operation, 1,401 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 https://deb.debian.org/debian bookworm/main amd64 libcrack2 amd64 2.9.6-5+b1 [44.0 kB]
Get:2 https://deb.debian.org/debian bookworm/main amd64 cracklib-runtime amd64 2.9.6-5+b1 [143 kB]
Get:3 https://deb.debian.org/debian bookworm/main amd64 libpwquality-common all 1.4.5-1 [51.3 kB]
Get:4 https://deb.debian.org/debian bookworm/main amd64 libpwquality1 amd64 1.4.5-1+b1 [12.8 kB]
Get:5 https://deb.debian.org/debian bookworm/main amd64 libpam-pwquality amd64 1.4.5-1+b1 [12.9 kB]
Fetched 264 kB in 0s (2,110 kB/s)
Selecting previously unselected package libcrack2:amd64.
(Reading database ... 29354 files and directories currently installed.)
Preparing to unpack .../libcrack2_2.9.6-5+b1_amd64.deb ...
Unpacking libcrack2:amd64 (2.9.6-5+b1) ...
Selecting previously unselected package cracklib-runtime.
Preparing to unpack .../cracklib-runtime_2.9.6-5+b1_amd64.deb ...
Unpacking cracklib-runtime (2.9.6-5+b1) ...
Selecting previously unselected package libpwquality-common.
Preparing to unpack .../libpwquality-common_1.4.5-1_all.deb ...
Unpacking libpwquality-common (1.4.5-1) ...
Selecting previously unselected package libpwquality1:amd64.
Preparing to unpack .../libpwquality1_1.4.5-1+b1_amd64.deb ...
Unpacking libpwquality1:amd64 (1.4.5-1+b1) ...
Selecting previously unselected package libpam-pwquality:amd64.
Preparing to unpack .../libpam-pwquality_1.4.5-1+b1_amd64.deb ...
Unpacking libpam-pwquality:amd64 (1.4.5-1+b1) ...
Setting up libpwquality-common (1.4.5-1) ...
Setting up libcrack2:amd64 (2.9.6-5+b1) ...
Setting up cracklib-runtime (2.9.6-5+b1) ...
Setting up libpwquality1:amd64 (1.4.5-1+b1) ...
Setting up libpam-pwquality:amd64 (1.4.5-1+b1) ...
Processing triggers for libc-bin (2.36-9+deb12u3) ...
Processing triggers for man-db (2.11.2-2) ...
pete42@pete42:~$
```

Password age control are configured in various files as shown in this section

Edit the file `/etc/login.defs` and set the values indicated below in red

```
#
# Password aging controls:
#
#      PASS_MAX_DAYS   Maximum number of days a password may be used.      30
#      PASS_MIN_DAYS   Minimum number of days allowed between password changes.  2
#      PASS_WARN_AGE   Number of days warning given before a password expires.  7
#
```

The above changes only affect new users, for existing users issue the command below once for each user i.e. pete42 and root

```
chage -M 30 pete42      ## existing user pwd expiration days
chage -m 2 pete42       ## existing user min days for pwd change
chage -W 7 pete42       ## existing user warn days of expiry
chage -M 30 root        ## existing user pwd expiration days
chage -m 2 root         ## existing user min days for pwd change
chage -W 7 root         ## existing user warn days of expiry
```

Edit the file `/etc/security/pwquality.conf` and set the values indicated below

```
#
#      minlen           Minimum number of characters for password          10
#      minclass         digits, uppercase, lowercase, others              3
#      maxrepeat        max repeat characters                             3
#      usercheck        username contained in password                    1
#      difok            Num chars in new pwd not present in old pwd        7
#      dcredit          Minimum 1 numeric digit                           -1
#      ucredit          Minimum 1 uppercase character                      -1
#      enforce_for_root - uncomment to enforce policy for root user
#
```

The above changes only affect new users, for existing users issue the command below once for each user i.e. pete42 and root

```
pete42@pete42:~$ sudo passwd pete42
[sudo] password for pete42:
New password:
BAD PASSWORD: The password contains less than 1 uppercase letters
New password:
Retype new password:
passwd: password updated successfully
pete42@pete42:~$
```

**NOTE** pete42 password changed to orbData\_00

**NOTE** root password should be set as well - it will need to follow the above password policy!!!!

