

Digital Forensics Tools & Techniques

COMP832

Kali Linux Installation & Use Instructions

For this course and later courses in the programme, we shall be utilising Linux for much of the technical and practical components. The distribution we shall use is Kali which is a Debian distribution but specifically designed for cyber security and computer forensics. As such, many of the security and forensics tools (software) are supplied with Kali, and many others can be simply installed to complement the native tools.

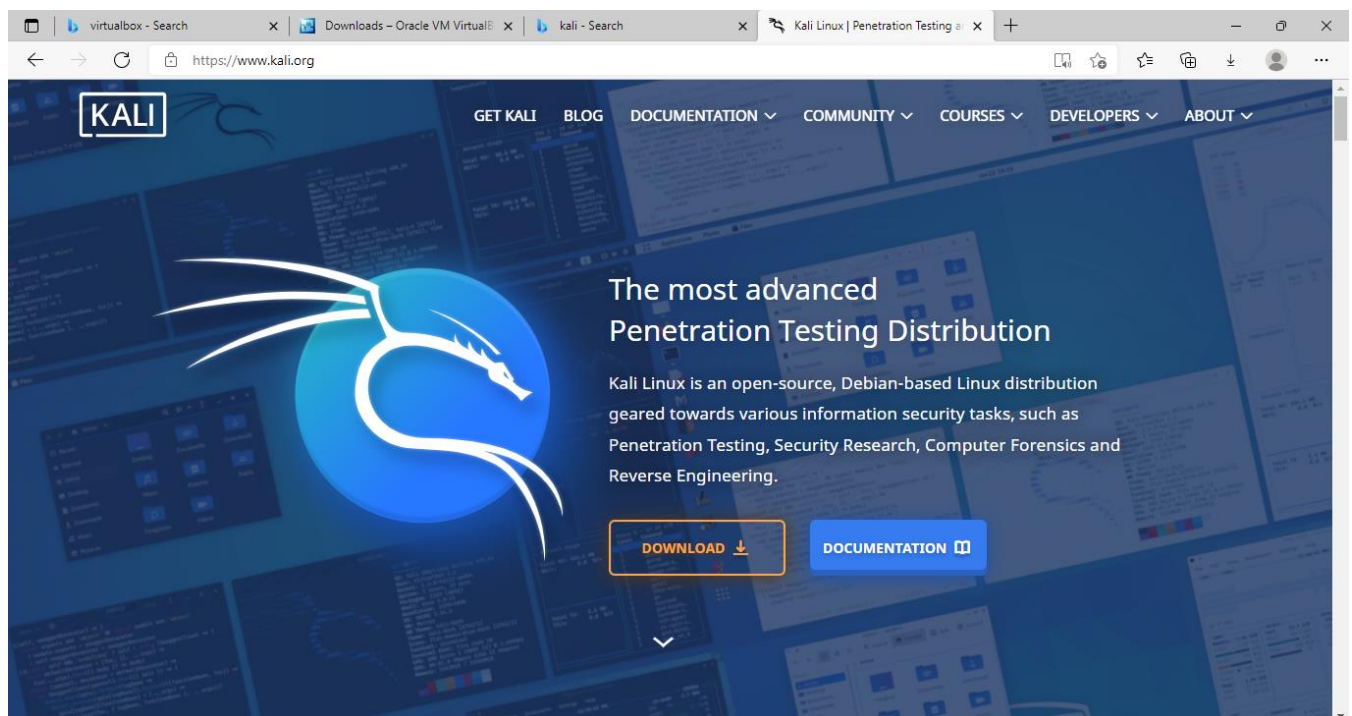
Kali can be used in several different methods and the choice will be yours as to how you use it. There are 3 methods that will be discussed and instructions on how to use all 3 follows. The 3 methods are Live, Virtually and Installed. This guide assumes you are using Windows and most screenshots are from Kali 2020 and Windows 10. You will need a spare USB stick – usually 8GB is big enough.

Note: Using a Virtual Machine is the preferred method, and I would recommend this if you use Kali only occasionally. Kali 2020 and Kali 2021 are significantly easier to use and more reliable in a Virtual Machine than earlier Kali versions. Using Kali Virtually also allows simple switching between Windows and Kali, dragging and dropping files between the 2 operating systems and the ability to create multiple instantiations of Kali, so you can easily begin a class again from an earlier version of your Kali instantiation – I shall explain in the course. The instructions for installing Kali are for an earlier version but I have updated the Virtual Machine installation instructions for Kali 2021.

Method 1: Kali Live

Live means that the operating system is booted from a USB stick. The version of Kali that we shall be using is the latest version available from the Kali web site <http://www.Kali.org>

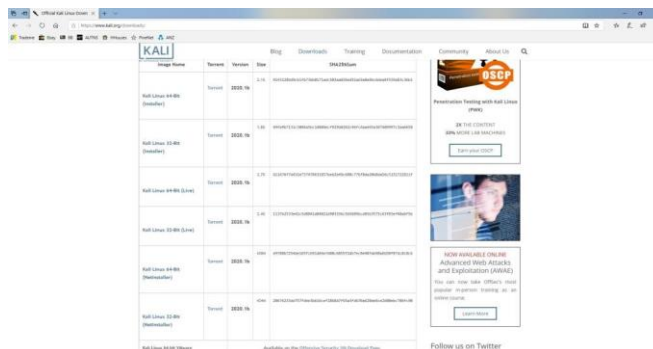
If you have an earlier version, that is fine and will work just as well but 2021 is more simple to use than earlier versions..



Select 'Get Kali' from the top menu bar:

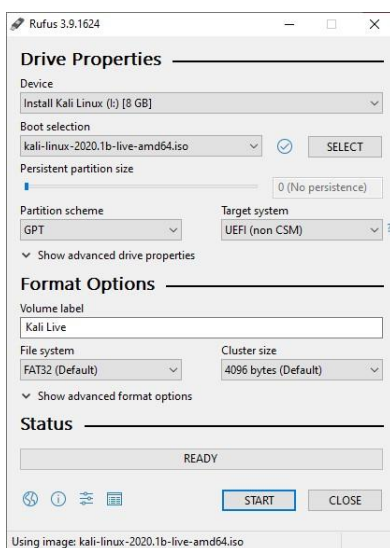
There are a number of different install files available with each (Installer – Live – NetInstaller) available in 32bit and 64bit versions. Ensure you know whether your computer is running as 32 bit or 64 bit.

To install the Live version, select 'Download' and then the Kali Linux 32 or 64 Bit (Live). You can download it as an ISO file or as a Torrent. If you wish to use the Torrent method, you will require a Torrent Downloader. There are many free Torrent downloaders and the choice is entirely yours as to which one you may wish to use. I downloaded "Free Torrent Download" but only because this came up first on a Google search.

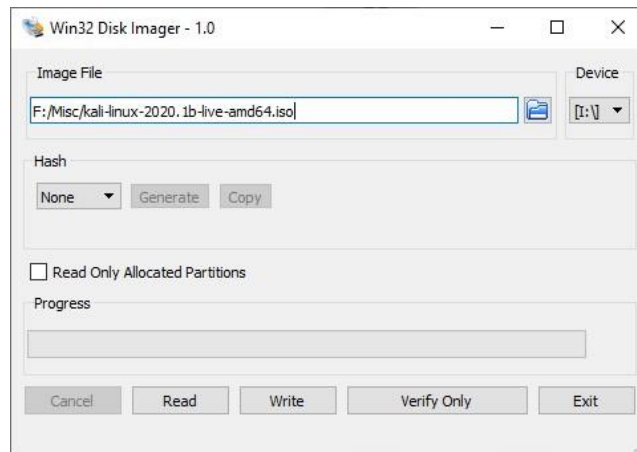


Once you have downloaded the ISO file, you now need to burn the ISO image to a USB stick. There are several tools available for this but the two I commonly use are Rufus and Win32DiskImager, both available for free download.

This is where things can get a bit complicated. Sometimes Rufus works best and sometimes Win32DiskImager works best, it depends on the computer you will be booting to. Therefore, if you try one tool and the computer will not recognise the USB stick when you attempt to boot, try the other tool and see if that works. Older computers did not utilise UEFI or 'Secure Boot' but most computers now do. If you have burnt the stick in Win32DiskImager, you do not have the choice for UEFI boot, but Rufus will allow this if you change the 'Partition Scheme' to GPT (rather than MBR). You may wish to start with Rufus using GPT and UEFI first rather than Win32DiskImager. If your computer has Secure Boot selected in the BIOS, you may need to disable secure boot and select Legacy Support Enabled. Each computer tends to be slightly different so a little trial and error is sometimes required. Some computer will not boot to Windows if secure boot is disabled, so you may prefer Rufus with GPT and UEFI boot first and if that does not work, Rufus with MBR.



If you are using Win32DiskImager, be aware that it will look for a .img file, but your downloaded Kali file will be a .iso file. You need to change the Disk Images in the bottom right corner to *.* so that it looks for all files.



Ensure the write to 'Device' is selected correctly. It must be the USB stick that you intend to burn the iso to, so check carefully that it is. If you accidentally write to your hard drive, you will damage the operating system and all files, so be careful.

Once the iso is burnt onto the USB stick, you can now try booting your computer from the stick. You will likely need to select the USB to boot to. First, you will need to enter the setup mode. Each computer is different, sometimes you need to press the delete key or the F12 key or the escape key or some other key. If you are not sure how to stop the computer at initial boot to enter the setup menu, you will need to Google it for your computer.

Once you have the initial menu, F9 will give the Boot Device Options. You need to select the USB stick with the Kali image on. If you get to the Kali screen, then the stick is booting. If not, and your original (Windows?) operating system boots, then your computer is not booting from the stick. Try again with different options (Rufus, Win32DiskImager and perhaps BIOS settings).



There are several menu choices for booting (this image is an older version of Kali). Live will boot to Kali but will not 'record' any changes to the stick, so if you install other software or enter commands in the Terminal, these will be lost when you shut down. Forensic mode is similar but prevents writing to any hard drive or USB stick that you may attach to the computer. Live USB Persistence will keep any changes you make to the software and record your commands which can be useful when you want to reuse older commands. I normally select Persistence mode for these reasons.

If all goes well, you will boot to the Kali Desktop. Kali 2020 looks a little different than earlier versions and one important difference is that Kali 2020 does not allow the user to boot to Root. Rather, the default username is kali and the password is kali. In older versions the username is root and the password is toor (root backwards). Root will give full access privileges but other users will not have full privileges. It is a little easier if you do boot to Root and there is a workaround for Kali 2020. This will be demonstrated at the end of this document.

Method 2: Running Kali Virtually

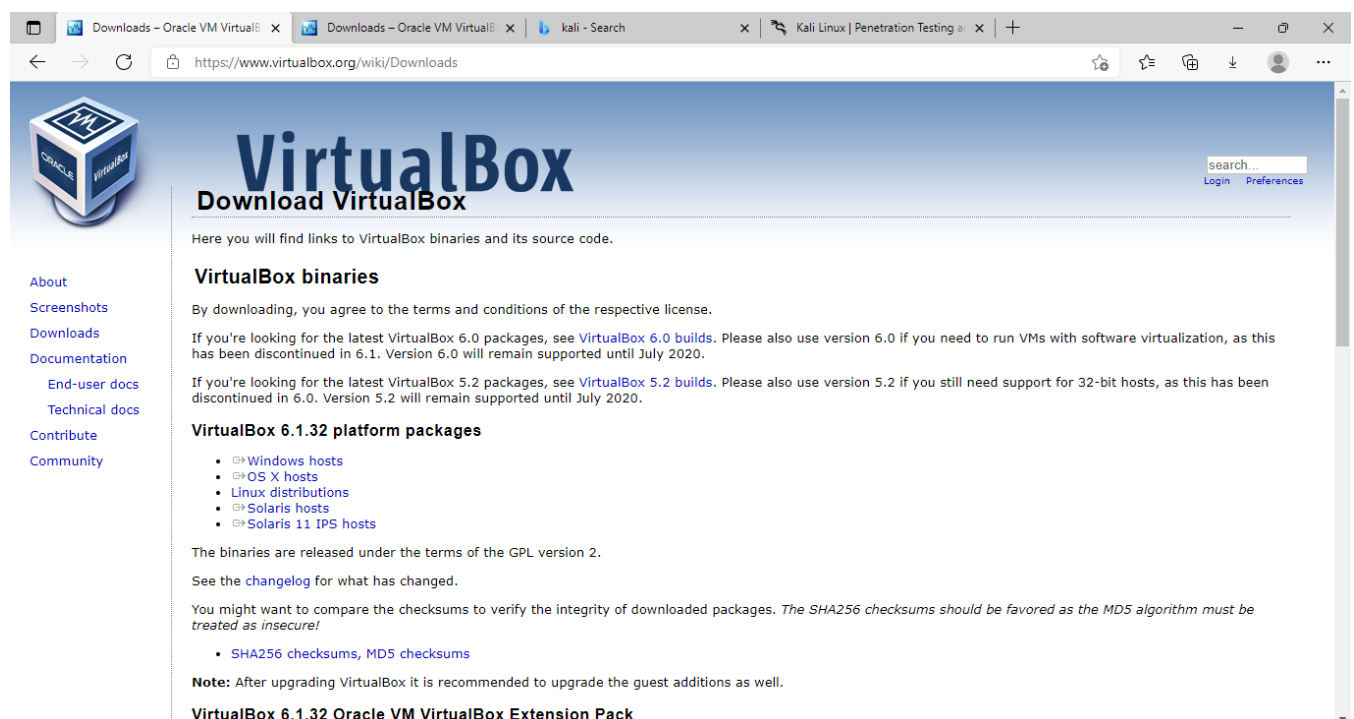
Virtual Machines make running other operating systems quite simple, but they can be a bit complex to get running correctly. You may also find that recognising external and internal drives can be difficult. VMs tend to either work flawlessly or cause endless technical issues but I have found the latest versions of Oracle VirtualBox and Kali 2021 tend to work well.

This guide will step through setting up Virtual Box and then installing Kali Linux in Virtual Box. The version of Kali is assumed to be Kali 2021 but an older version is fine to use. You may use any virtual machine you wish but please bear in mind that if you need assistance and you have chosen to use other software than that demonstrated here, it is unlikely that I will be able to assist as I probably won't have experience with your other choices of software. Therefore, I would recommend Oracle Virtualbox for simplicity.

Type into your browser the url <http://www.virtualbox.org>

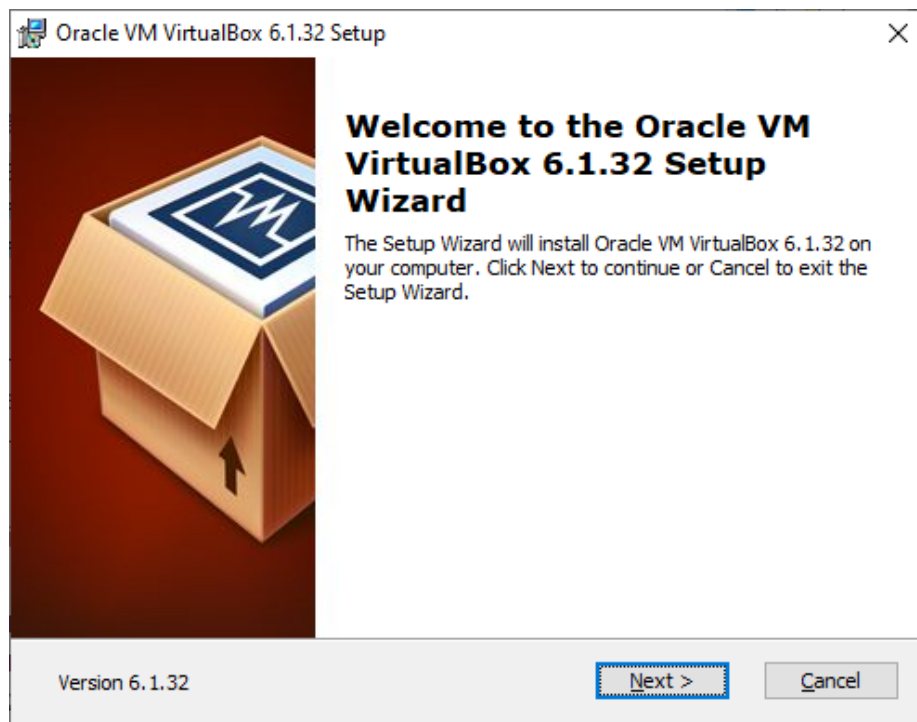


And select 'Download VirtualBox 6.1



And then Select 'Windows Hosts'.

The download of the 103MB file should begin. Once it has downloaded, open the file and install VirtualBox.



And if all goes well....

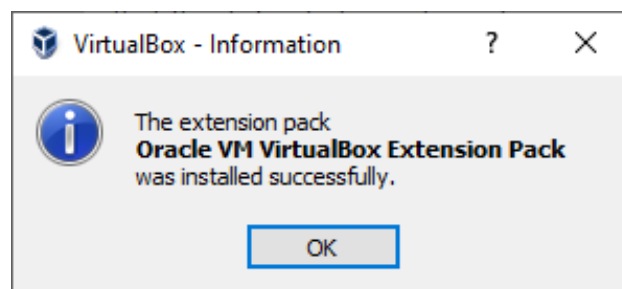
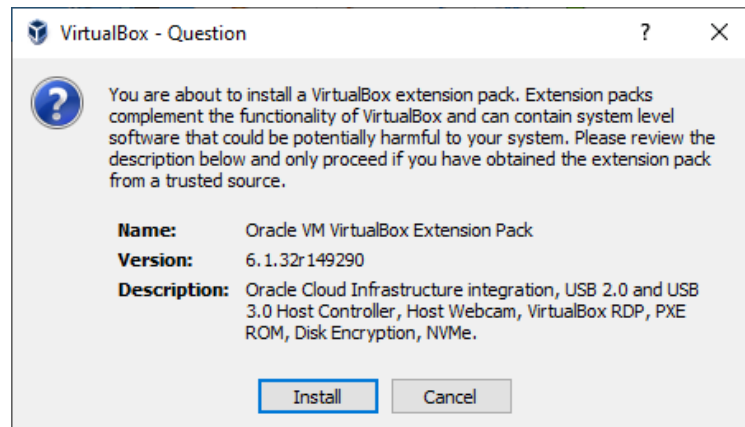


If you start VirtualBox you will see the following screen. However, we need to install the VirtualBox expansion pack, so close VirtualBox and install this from the VirtualBox site, located just under the 'Windows Hosts' link.

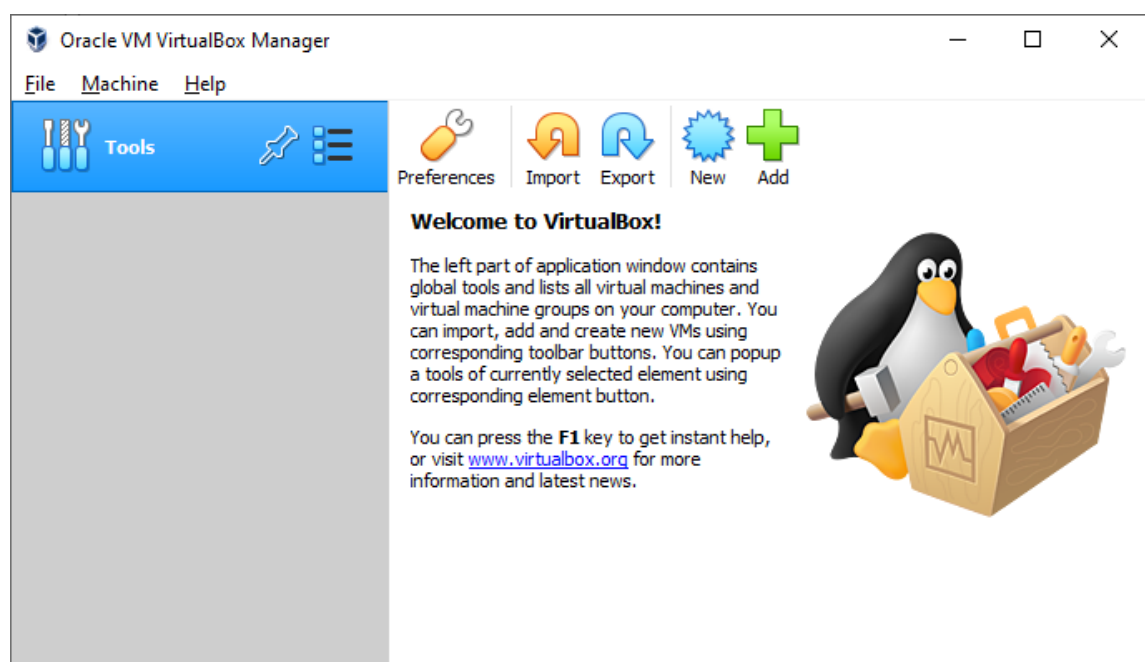
[VirtualBox](#) 6.1.32 Oracle VM VirtualBox Extension Pack

- [All supported platforms](#)

This is a 10MB file that we need to run to install the extensions. Install the extensions.

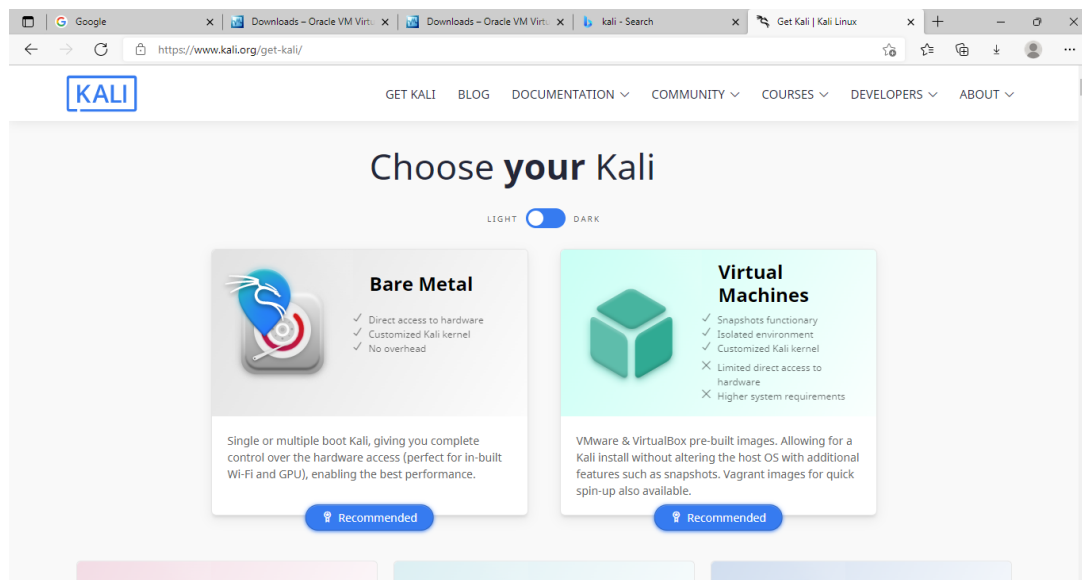


If we now run VirtualBox on our computer, we get the following startup screen.



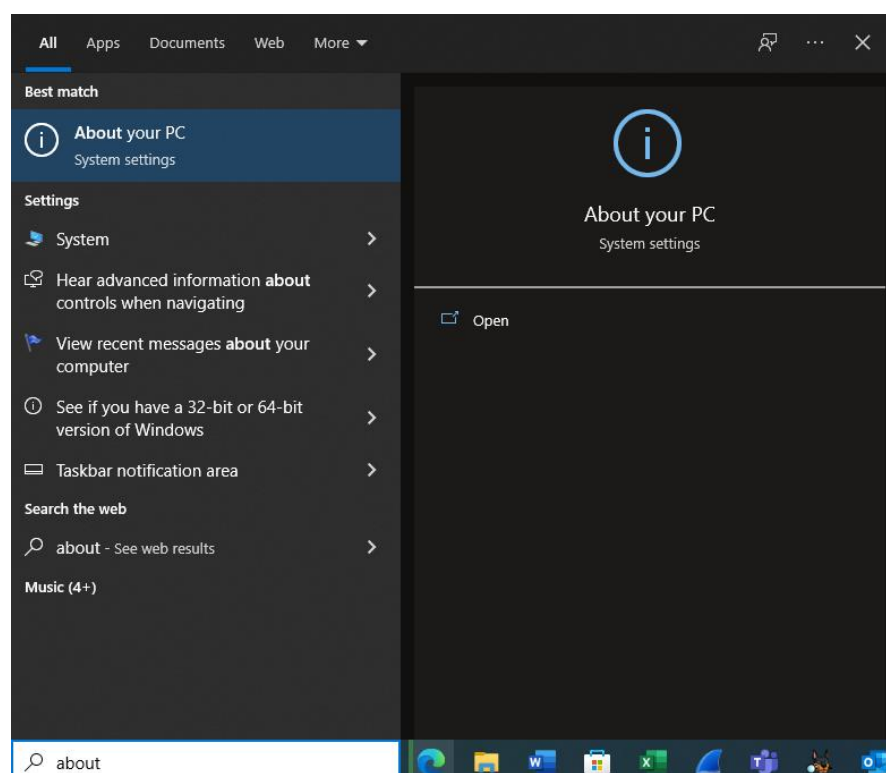
On the left is where the instantiations (appliances) of Kali will be installed. There are currently none there as we need to download and import one. Here we have a choice: we can either do a full install of a Kali ISO (similar to method 1) and install Kali ourselves which will take some time – perhaps 30 minutes – and then configure Kali for our use, or we can rely on the good folks at Kali who have created a snapshot of Kali and save it as one large file – 3.2GB. The second method ends with the same result as the first but is quick and simple, so we shall do that.

The next step is to install Kali in the VirtualBox. Kali has developed an install package specifically for VirtualBox and this is the file you should download from the Kali web site. On the Kali web site select 'Get Kali' from the top menu bar. On the right is 'Virtual Machines' so select this option.

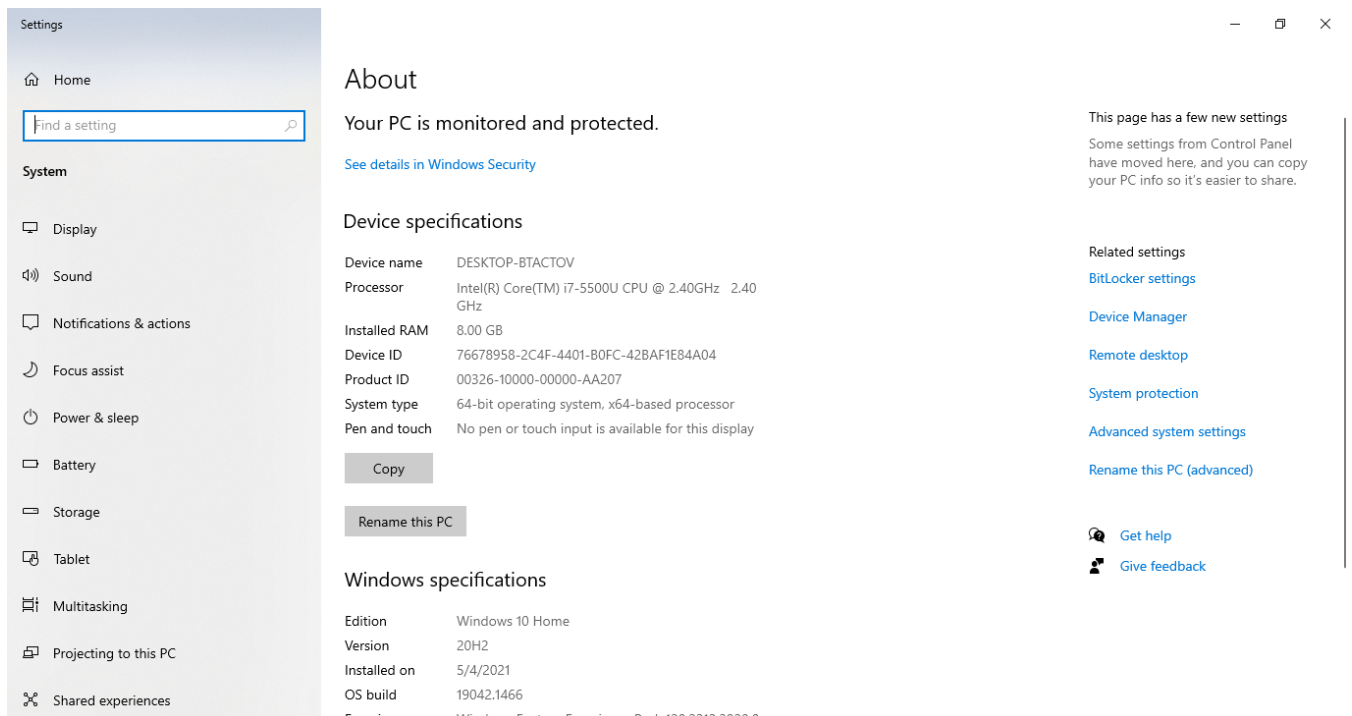


Then select either the 32 bit or 64 bit version depending on which of these Windows operating systems you are using.

To find this information on your computer (Assuming Windows 10) type 'about' into the computer search box.

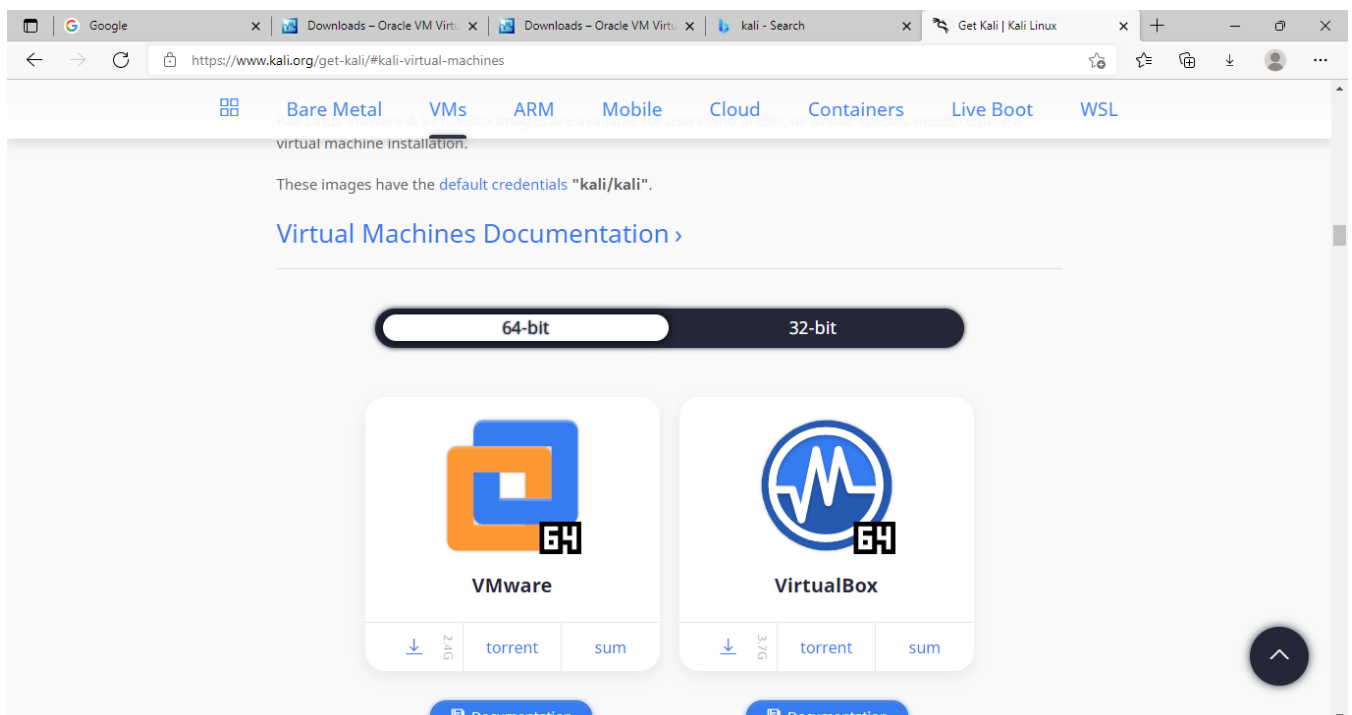


And then select 'Open'



I have Windows 10 64 bit.

Select 'VirtualBox' on the right (Not VMware')

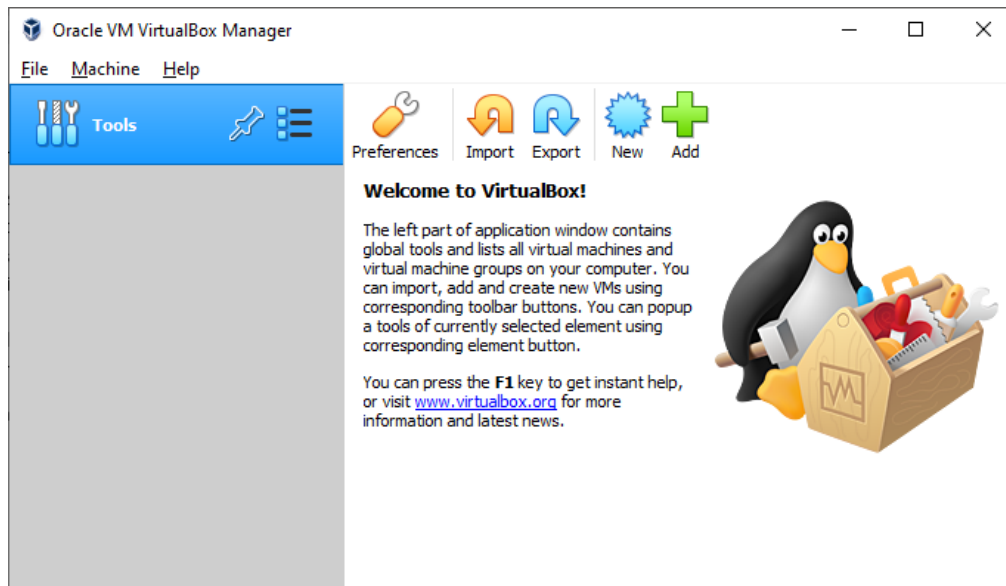


This will download the Kali VirtualBox snapshot – kali-linux-2021.4a-virtualbox-amd64.ova

The .ova file is called an appliance (Oracle VirtualBox Appliance) and it can be imported into VirtualBox so that Kali is ready to use. It is 3.6GB and depending on your Internet connection speed could take an hour or more to download. Once downloaded, we can import this file (appliance) into VirtualBox

and we can import it multiple times if we wish to have multiple copies of Kali in the VirtualBox environment. This is useful if you are demonstrating installing additional tools in Kali and then wish to demonstrate the same process again. If the tools are already installed, they can't be reinstalled, but with another import of Kali, you can start with a fresh copy with none of the tools installed.

Once the .ova file has downloaded, start VirtualBox and select 'Import'.



Select the folder on the left of the following screenshot and locate the .ova file – probably in the Downloads folder.

← Import Virtual Appliance

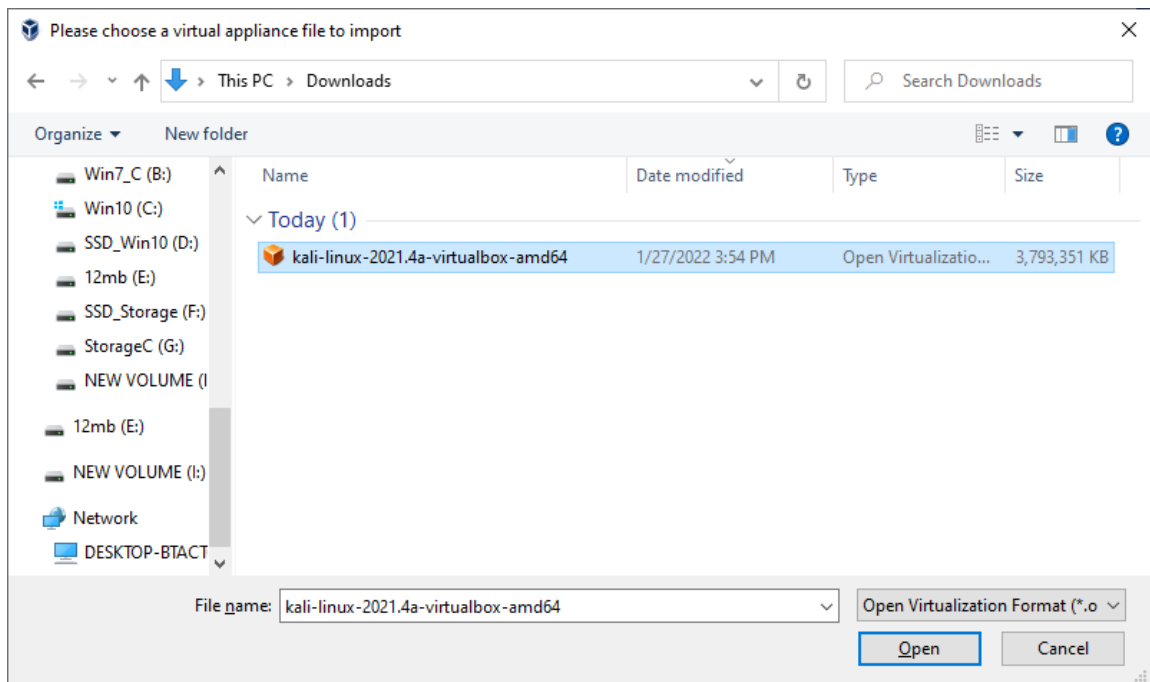
Appliance to import

Please choose the source to import appliance from. This can be a local file system to import OVF archive or one of known cloud service providers to import cloud VM from.

Source:

Please choose a file to import the virtual appliance from. VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below.

File: 

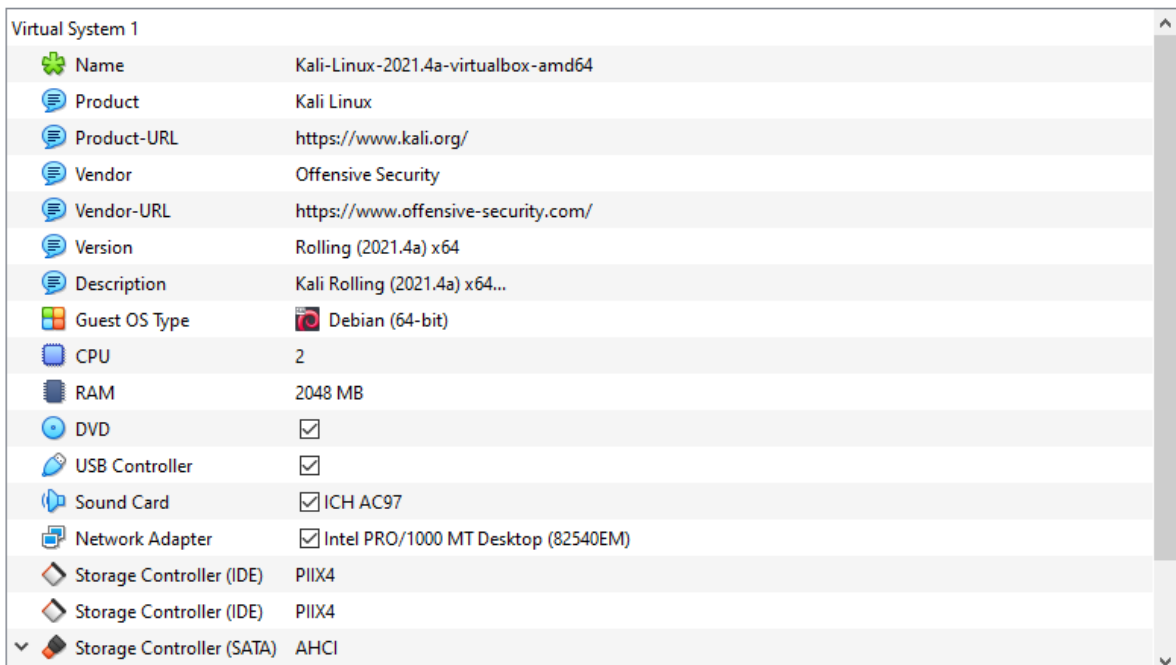


Leave the default settings and select 'Import'.

← Import Virtual Appliance

Appliance settings

These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.



Machine Base Folder: C:\Users\Misdf_1_Win10\VirtualBox VMs

MAC Address Policy: Include only NAT network adapter MAC addresses

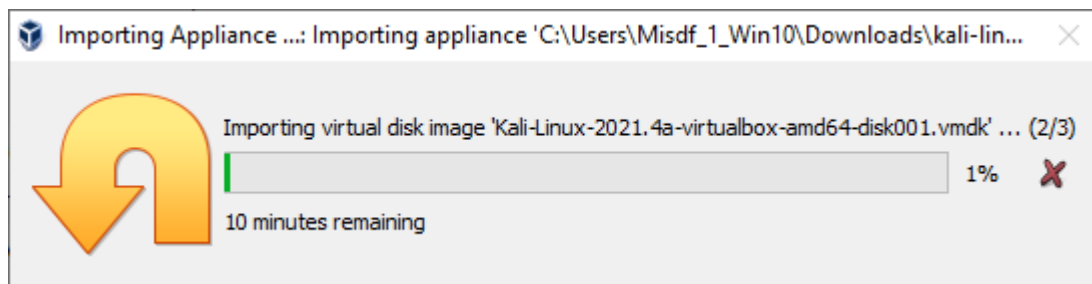
Additional Options: ☒ Import hard drives as VDI

Appliance is not signed

Restore Defaults

Import

Cancel



It will take a few minutes. You can change the name of the appliance, import it multiple times and delete the appliance at any time. You can also copy a Kali appliance after it is imported and doing this as a backup is a good idea. Select the 'Clone' option (Dolly the sheep) and then 'full clone' to make an exact copy. I shall make a backup clone called Kali_2.

? X

← Clone Virtual Machine

New machine name and path

Please choose a name and optionally a folder for the new virtual machine. The new machine will be a clone of the machine **Kali-Linux-2021.4a-virtualbox-amd64**.

Name:

Path:

MAC Address Policy:

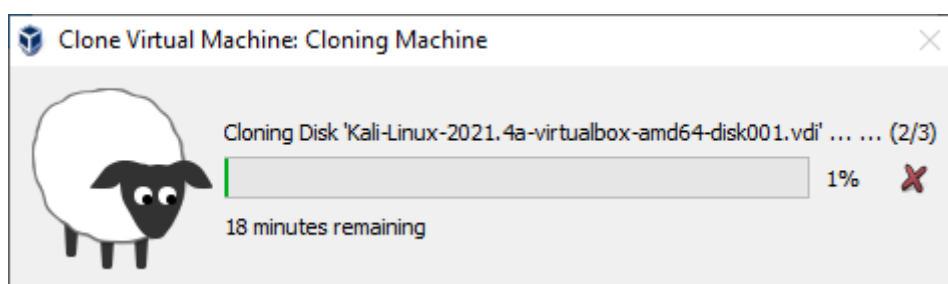
Additional Options: ☐ Keep Disk Names

☐ Keep Hardware UUIDs

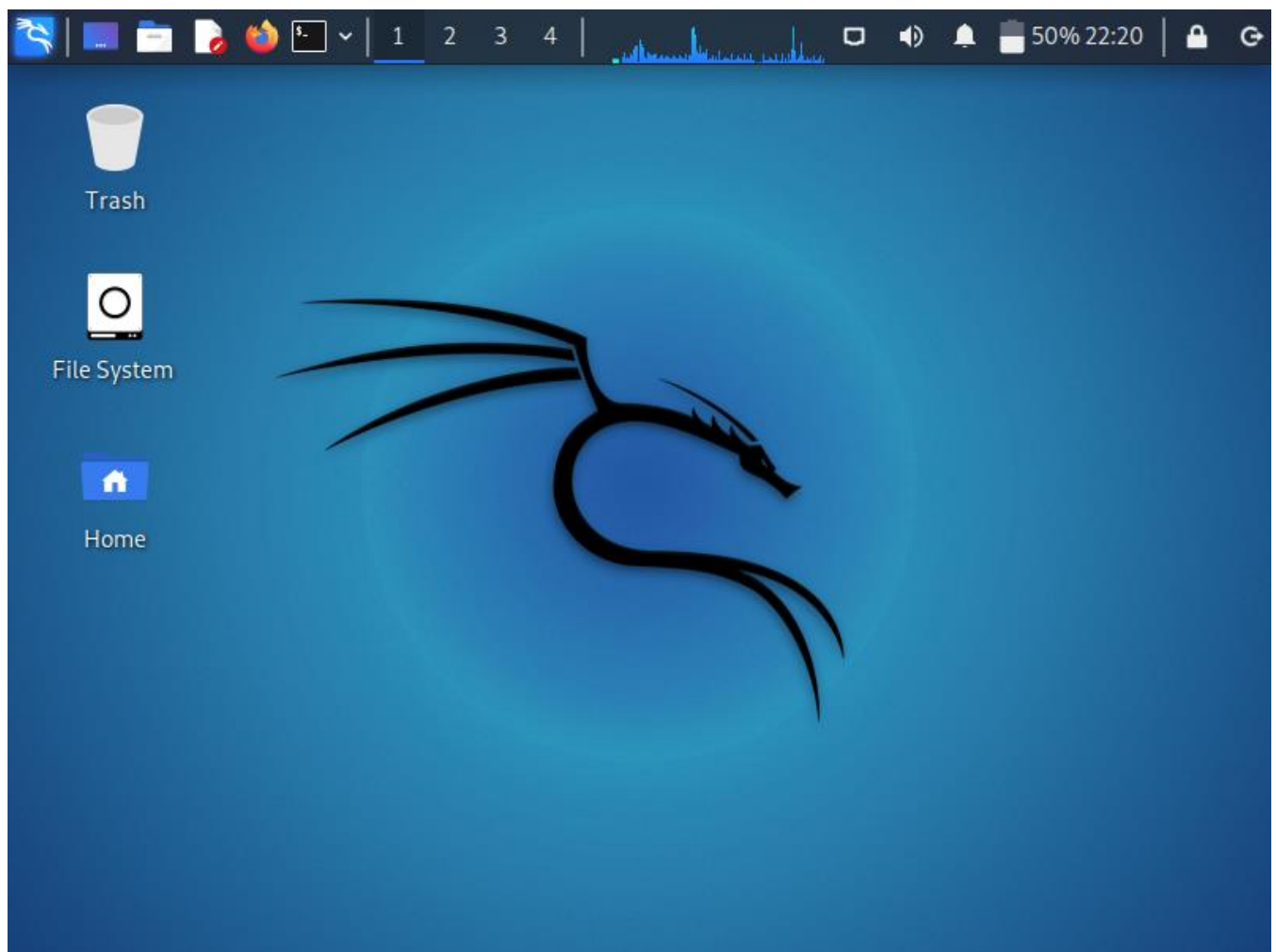
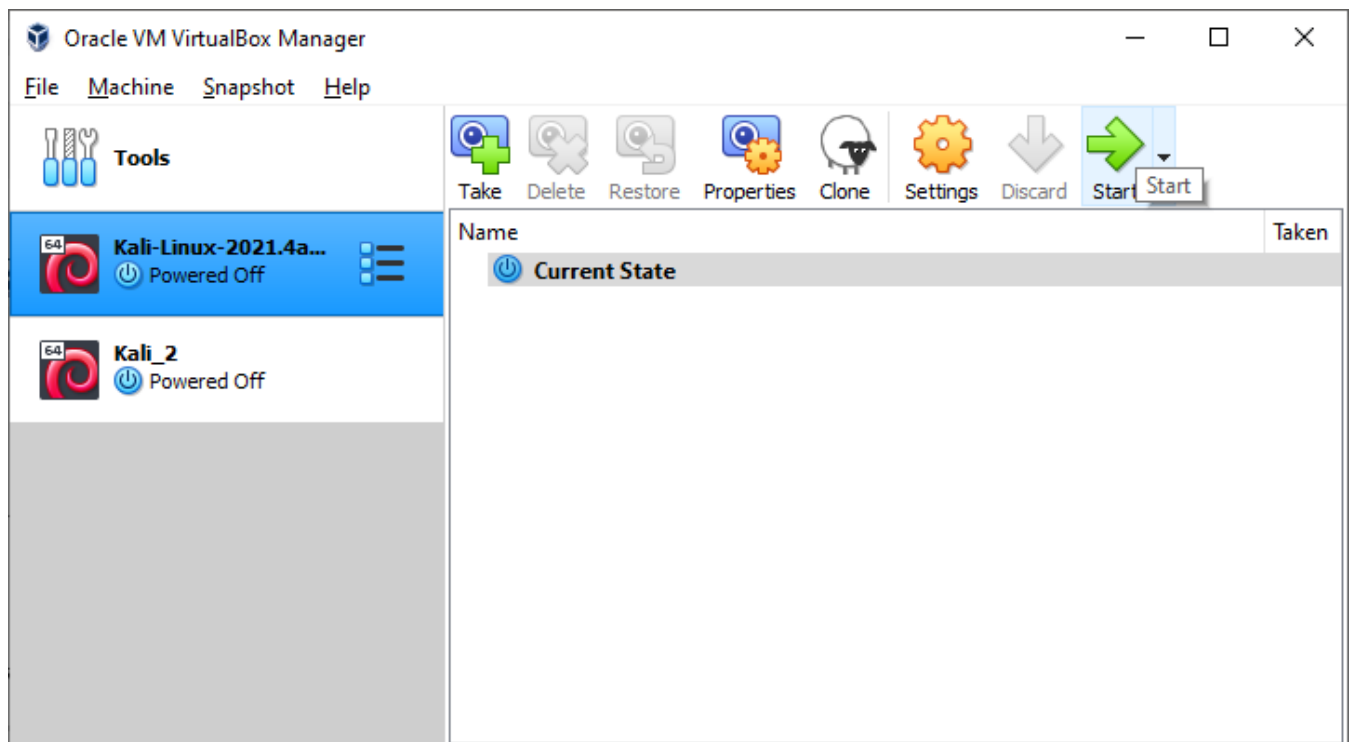
Expert Mode

Next

Cancel



I can now 'start' the original copy and log in with kali kali.




I can change the 'View' to full screen mode.

I shall then make a root account with the password kali using the following 2 commands in a Terminal (window).

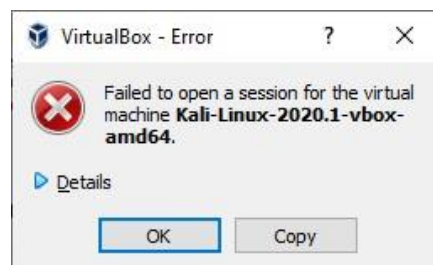
```
>sudo su
```

```
>passwd root
```

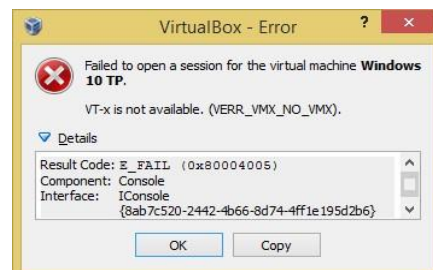


```
kali@kali: ~  
File Actions Edit View Help  
kali@kali:~$ sudo su  
We trust you have received the usual lecture from the local System  
Administrator. It usually boils down to these three things:  
  
#1) Respect the privacy of others.  
#2) Think before you type.  
#3) With great power comes great responsibility.  
  
[sudo] password for kali:  
root@kali:/home/kali# passwd root  
New password:  
Retype new password:  
passwd: password updated successfully  
root@kali:/home/kali#
```

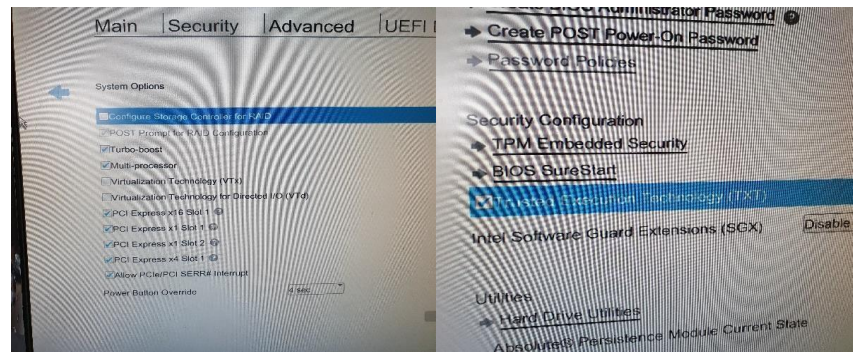
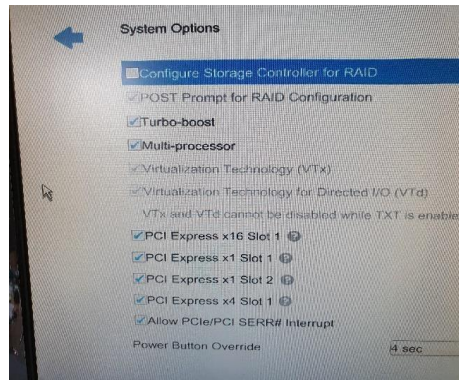
Once it is imported, Kali is ready to use. The default username and password is 'kali'. You will see that it is 'powered off' and you can either select Start or double click Kali. However, one issue may become apparent. You may get an error message like the one below. If so, select 'Details' and see what it relates to.



The error I received was similar to this one:



This related to 3 BIOS settings that needed to be switched on to allow the VirtualBox to utilise the computer's CPU. VTx and VTd needed to be selected (under Advanced) and this then allowed TXT to be selected which was under the Security tab. If you have an error, it may be different, and you will need to read the details and see what needs configuring. When I changed the BIOS settings and rebooted, Kali then ran in VirtualBox without any issues.



When running Kali, there is a protection built into the commands that don't allow any changes to the system unless you are either logged in as the 'root' user or you type sudo (superuser does) before the command. I find typing sudo constantly a little frustrating, so I create a root account and always log in as root – not necessarily a good habit but this may make things a bit easier for the class. Read below for how to create a root account and password. Remember to log out and then log in again as root.

That's it – you are now ready to use Kali in a Virtual Machine. It is simple to shut down kali and you can 'power off the machine' where anything you have done, including installing any tools, will be lost, or you can 'save the machine state' when you power off and this will save all the changes you have made. Generally, I 'save the machine state' unless I don't want to save the changes. If you save the machine state, you will not need to log in next time you use Kali as it boots up to where you left off.



Method 3: Installing Kali on a Computer

If you wish, you can download the Kali Linux Installer (not the Live download) and install Kali as your operating system. It can run alongside Windows as a dual boot but can be quite tricky to configure. You also need to be careful that you do not corrupt your other operating system when you are trying to install Kali and for this reason I would not recommend installing Kali on a computer unless you are either very confident with Linux or you have a spare computer that you can use that can be reinstalled if things go wrong.

To make this very clear: I do not recommend installing Kali as a standalone operating system. It is not necessary for the programme and can sometimes result in significant issues, both with the Kali installation and with any other operating system you may have on your computer.

Kali 2020 Configuring Root Access:

The screenshot below shows Kali 2020. Earlier versions have a menu down the left side. These versions also default to root access which gives full access privileges and also means that 'sudo' (super user does) is not needed before many commands. The reason Offensive Security gives for not allowing root access is that users could sometimes enter commands that would damage their operating systems or hard drives without realising what they were about to do. However, we shall be using root privileges frequently and you can either utilise sudo before commands or log on as root with this workaround for Kali 2020.



The screenshot below shows the commands in a terminal to configure a password for root. A terminal is similar to a DOS window in Windows and allows commands to be entered directly by command line. If you enter these 2 commands, you can configure a password for root. Normally,toor is used as the root password (it is root backwards) but you can choose any password. The password will not appear as you enter it here.

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali:~$ sudo su  
  
We trust you have received the usual lecture from the local System  
Administrator. It usually boils down to these three things:  
  
#1) Respect the privacy of others.  
#2) Think before you type.  
#3) With great power comes great responsibility.  
  
[sudo] password for kali:  
root@kali:/home/kali# passwd root  
New password:  
Retype new password:  
passwd: password updated successfully  
root@kali:/home/kali#
```

Updates and Installing Packages Issue:

Updating Kali (updates, not a later version) and installing additional tools (software similar to apps) is very simple in Linux. The command (assuming you are logged on as root so no 'sudo' required) is apt-get and then the name of the tool. We shall need to install several tools that are not included with every version and so you will need to ensure that you can do so.

You may find that if you try to update Kali with the command 'apt-get update' or try to install additional tools, such as 'dcfldd' with the command 'apt-get install dcfldd', you get the following screen.

```
Shell No.1  
File Actions Edit View Help  
root@kali:~# apt-get install dcfldd  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
E: Unable to locate package dcfldd  
root@kali:~#
```

This indicates that Kali is not finding the web site link to download the tool. This is likely because the text file containing the web addresses is either empty or has lines commented out with a # before the address. A hash tells Kali to ignore the line. You will therefore need to update this text file (called sources.list) so that Kali can find the tools. To do this, use a text file editor. Nano should be included in Kali. There are others that are easier to use but you may need to install them after this fix, so try nano. Leafpad is easy to use but in the screenshot below you can see that Kali failed to find it. The bottom line is the command to edit the sources.list file located in /etc/apt/

```
Shell No.1
File Actions Edit View Help

root@kali:~# apt-get install dcfldd
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package dcfldd
root@kali:~# leafpad /etc/apt/sources.list
bash: leafpad: command not found
root@kali:~# nano /etc/apt/sources.list
```

You should see that the file contains entries similar to the screenshot below. I have removed the # before each of the 4 lines so that Kali will now follow the link. To save the file in nano, control o (oh not zero). If the sources.list is empty, you will need to type in the 2 deb lines that contain 'kali rolling'.

```
Shell No.1
File Actions Edit View Help
GNU nano 4.5 /etc/apt/sources.list Modified

deb cdrom:[Kali GNU/Linux 2020.1rc4 _Kali-last-snapshot_ - Official amd64 DVD Binary-1 with firmware 20200124-09:35]/ kali-rolling main non-free
deb cdrom:[Kali GNU/Linux 2020.1rc4 _Kali-last-snapshot_ - Official amd64 DVD Binary-1 with firmware 20200124-09:35]/ kali-rolling main non-free
deb http://http.kali.org/kali kali-rolling main non-free contrib
deb-src http://http.kali.org/kali kali-rolling main non-free contrib

# This system was installed using small removable media
# (e.g. netinst, live or single CD). The matching "deb cdrom"
# entries were disabled at the end of the installation process.
# For information about how to configure apt package sources,
# see the sources.list(5) manual.

File Name to Write: /etc/apt/sources.list
^G Get Help      M-D DOS Format  M-A Append     M-B Backup File
^C Cancel        M-N Mac Format  M-P Prepend    To Files
```

Once you have saved this file and exited nano (ctrl x) you must then update Kali or it will not look for the file changes. To do this, in a terminal type:

apt-get update

or sudo apt-get update (if you are not a root user).

Then try installing additional software tools.

Below is installing dcfldd with success now.

You can try installing leafpad, dc3dd and a tool I use for reading and writing microchips is flashrom (if you wish to try microchip reading with the necessary hardware).

```
Shell No.1
File Actions Edit View Help

root@kali:~# apt-get install dcfldd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  dcfldd
0 upgraded, 1 newly installed, 0 to remove and 865 not upgraded.
Need to get 43.2 kB of archives.
After this operation, 105 kB of additional disk space will be used.
Get:1 http://hlmel.fsmg.org.nz/kali kali-rolling/main amd64 dcfldd amd64 1.7-1 [43.2 kB]
Fetched 43.2 kB in 1s (32.1 kB/s)
Selecting previously unselected package dcfldd.
(Reading database ... 273432 files and directories currently installed.)
Preparing to unpack .../dcfldd_1.7-1_amd64.deb ...
Unpacking dcfldd (1.7-1) ...
Setting up dcfldd (1.7-1) ...
Processing triggers for man-db (2.9.0-2) ...
Processing triggers for kali-menu (2020.1.7) ...
root@kali:~#
```

That's it.

Hopefully you have one of these 3 methods working. If it does not go well, and occasionally it does not, it can be very time consuming and very, very frustrating.

If you are really stuck with things, feel free to email me and I shall assist if I can.

Alastair anisbet@aut.ac.nz