Lab – Creating a Kali Live (Forensic Mode) VM Using VirtualBox

Overview

In this lab, you will learn how to create a Kali Live (Forensic Mode) VM Using VirtualBox. You will also learn why this is important.

In Live (Forensics Mode), the Kali operating system does not mount the suspect's hard drives, thereby Kali does write or leave any metadata or changes to the host's system.

A forensic image (forensic copy) is a bit-by-bit, sector-by-sector direct copy of a physical storage device, including all files, folders, and unallocated, free and slack space. Forensic images include not only all the files visible to the operating system but also deleted files and pieces of files left in the slack and free space.

Forensic imaging is one element of computer forensics, which is the application of computer investigation and analysis techniques to gather evidence suitable for presentation in a court of law.

This process is critical when digital evidence will be admitted as evidence in litigation as any change to the suspect's data made during the imaging process can make the evidence inadmissible in a court of law.

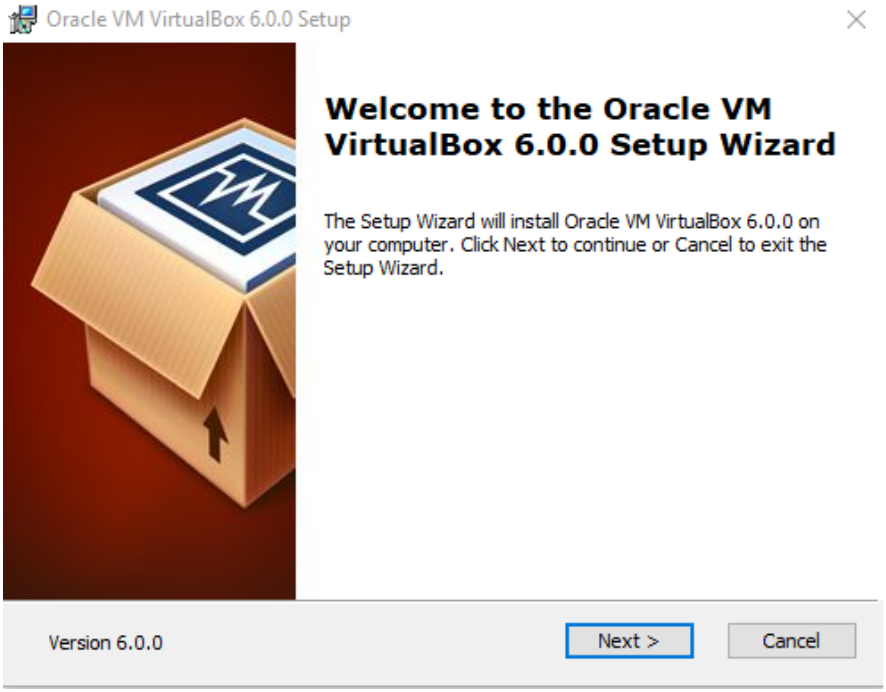
Lab Requirements:

1. **Be sure to review the lab before you begin**
2. Kali Linux ISO Image
3. VirtualBox
4. CPU that supports Virtualization.
5. 8GB of RAM preferred. (4 GB of RAM will Suffice but is not optimal)
6. At least 60 GB of free hard drive space. (An external hard drive or thumb drive can also be used as storage)

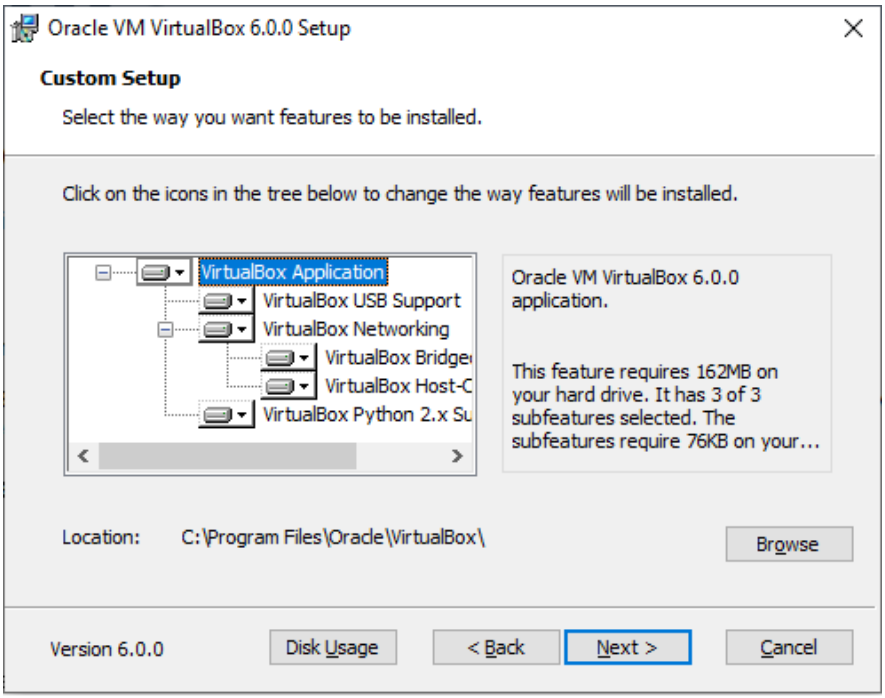
Download VirtualBox

Once you've downloaded VirtualBox, you can browse to the saved download location and run the installer. In this lab, I demonstrate installing VirtualBox, Version 6.0 but regardless of the version, the installation wizard remains intuitive.

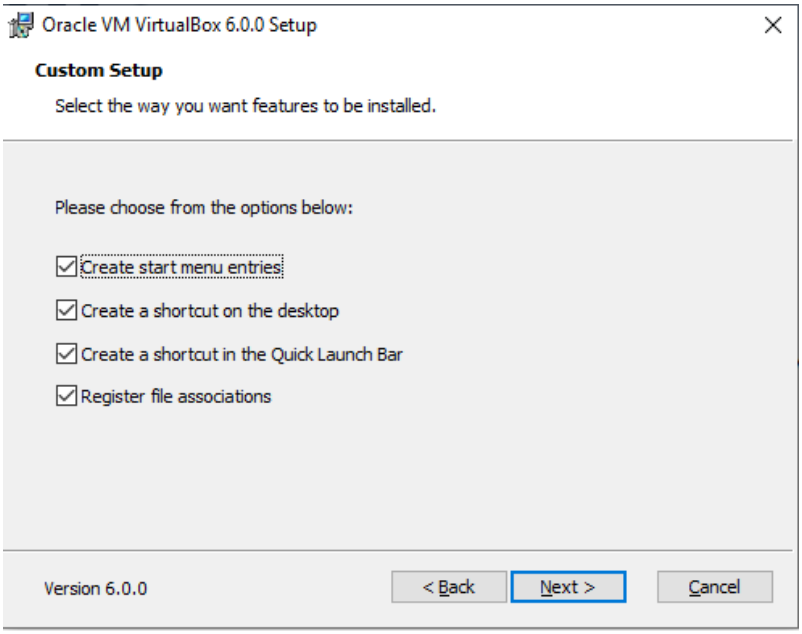
On the opening screen, click next.



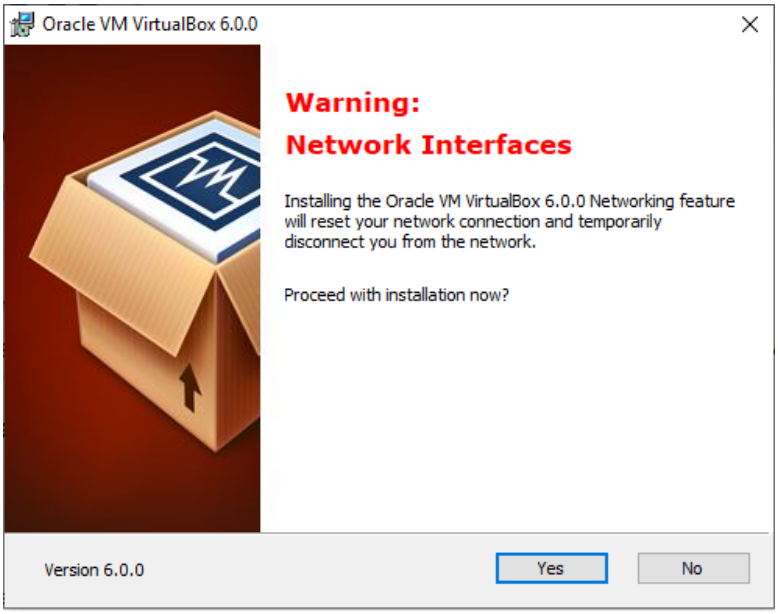
On the next screen, accept the defaults and click next.



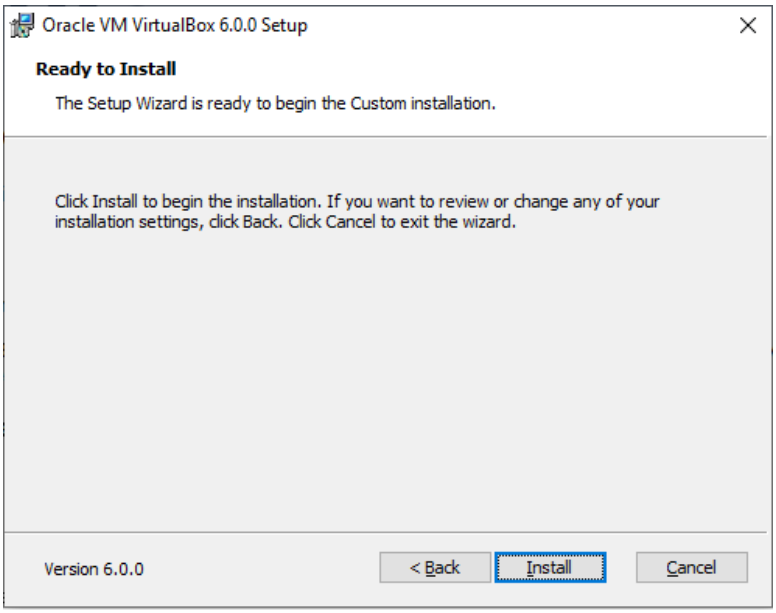
On the next screen, accept the defaults and click next.



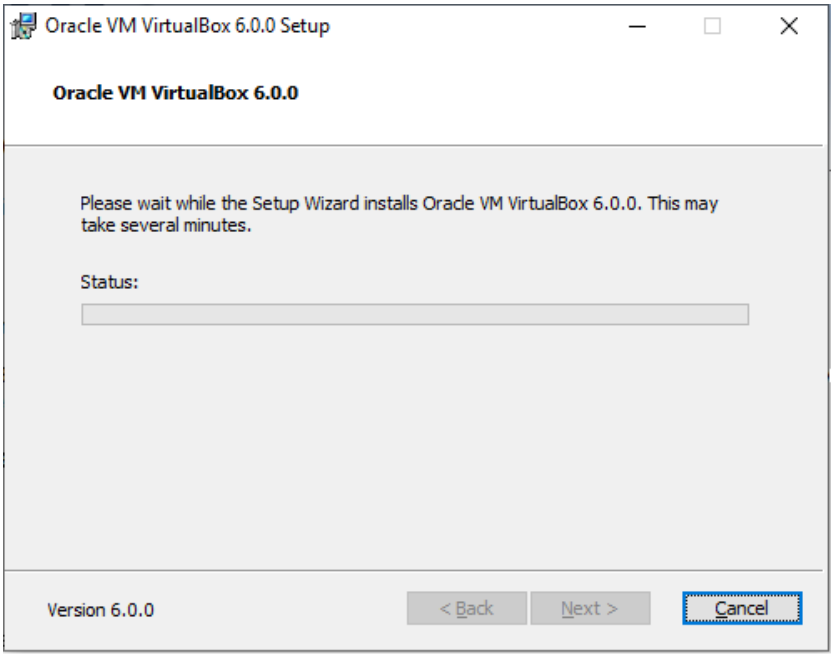
On the next screen, accept the warning and click Yes.



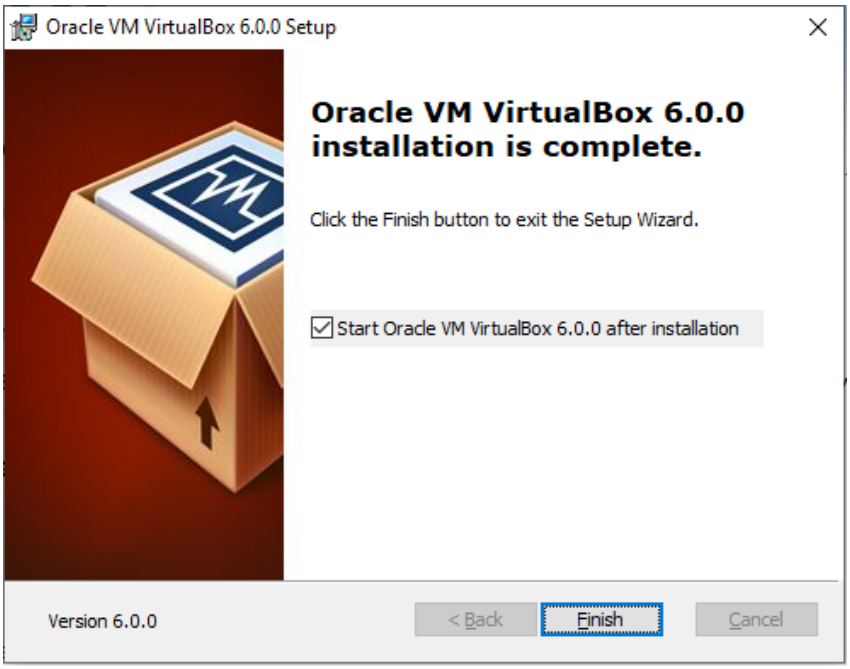
On the Ready to Install screen, click the install button.



The installation begins.



On the finish screen, click the Finish button and if prompted, restart your host machine.



Using Kali Live (Forensic Mode)

In this course, we will be simulating acquiring a forensic image. Throughout the course, different images will be provided for gaining experiencing using the different forensic tools and techniques presented in this course. Normally the suspect's hard drive(s) would be removed, documented, photographed, secured and transported to a forensic lab for analysis. Once inside the lab, the suspect's hard drive(s) would be attached to a hardware write blocker and a forensic image would be created for later analysis.

Here's a short presentation on connecting a suspect's hard drive to a hardware write blocker.

Forensic Data Acquisition - Hardware Write Blockers

It's important that you make the coloration between how we simulate using a software write blocker in this lab and how a hardware write blocker is used when seizing a suspect's hard drive in a real computer forensics case. But….

When a suspect's hard drive cannot be removed from the suspect's computer or laptop for whatever reason, then a Live CD and a software write blocker can be used to create a bit-by-bit forensic image of the suspect's hard drive(s).

In this course, we will be using a variety of small image files to simulate a suspect's seized hard drive. These small image files are attached as virtual hard drives in the storage settings of our Kali Linux Live CD virtual machine.

We will launch the virtual machine for Kali Linux using a Kali Linux ISO image. As the VM boots, we will attach the ISO image of Kali Linux to the VM and as Kali Linux boots, we select the **Live Kali (forensic Mode)** from the boot menu.

In the real world, the ISO image would be burnt to a DVD or USB thumb drive and the suspect's machine would be made to boot from the DVD drive or the USB device.

Once we have a Kali desktop, we will create a forensic image using a software write blocker using Kali's command line or terminal. This process will be repeated with each forensic lab as needed.

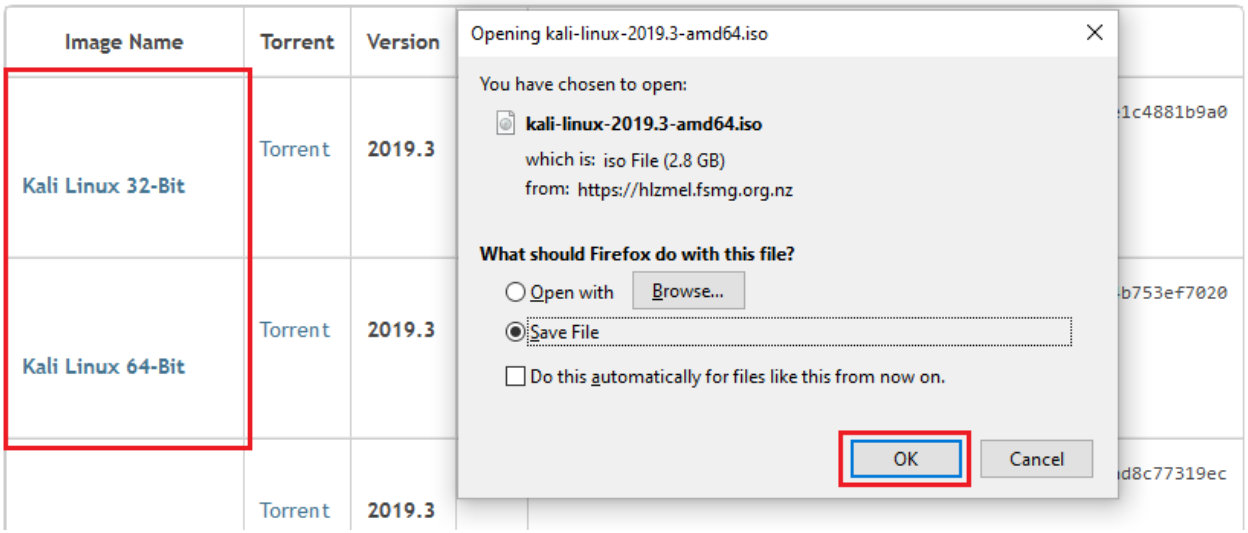
Why we use the Live Kali (forensic Mode) Option

It's non-destructive — it makes no changes to the host system's hard drive or installed OS, and to go back to normal operations, you simply remove the "Kali Live" DVD or USB drive and restart the system.

Download the Kali ISO Image

We next need to obtain the ISO image for the Kali Live CD. Point your browser to the Kali image download site located at https://www.kali.org/downloads/

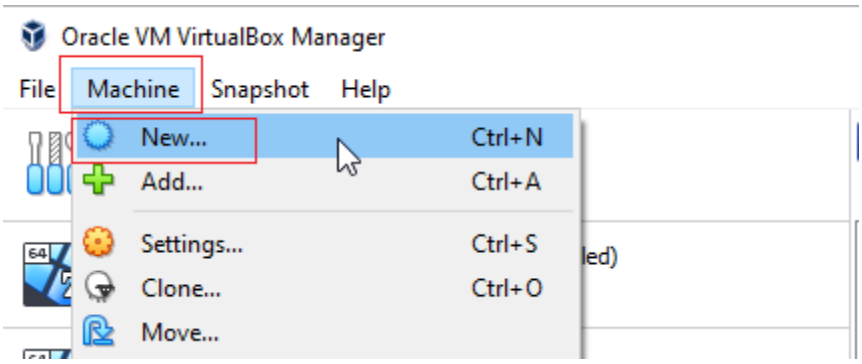
Depending on your hardware, you'll want to download the correct version depending on your hardware type, either 32-bit or 64-bit. I recommend that you use the direct download and not the torrent option. The torrent option can sometimes pull in files that are corrupted from one of the many torrent peers.



Save the image to a location on your machine.

Launch Kali in Live Forensic Mode

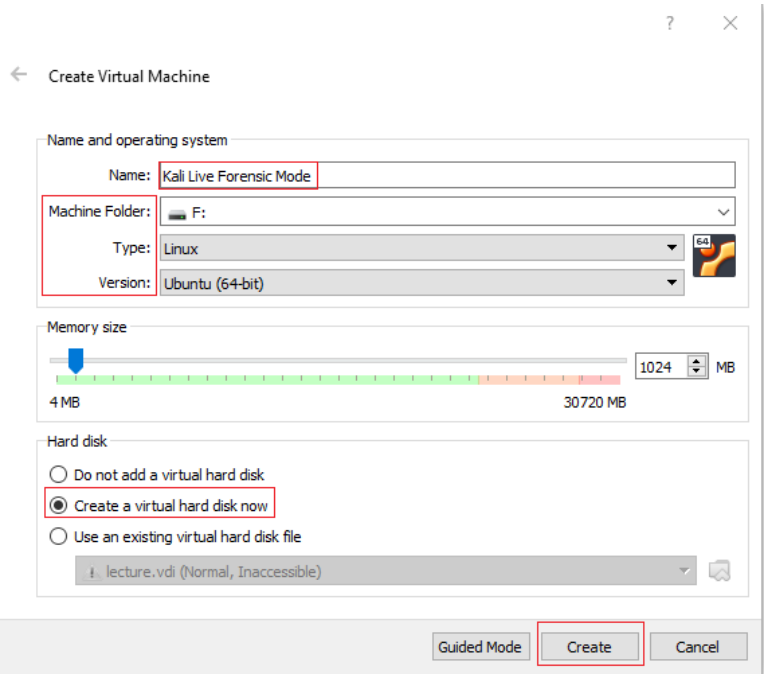
Open your install of Virtual Box Manager and from the overhead taskbar, click on **Machine** and from the context menu, select **New**.



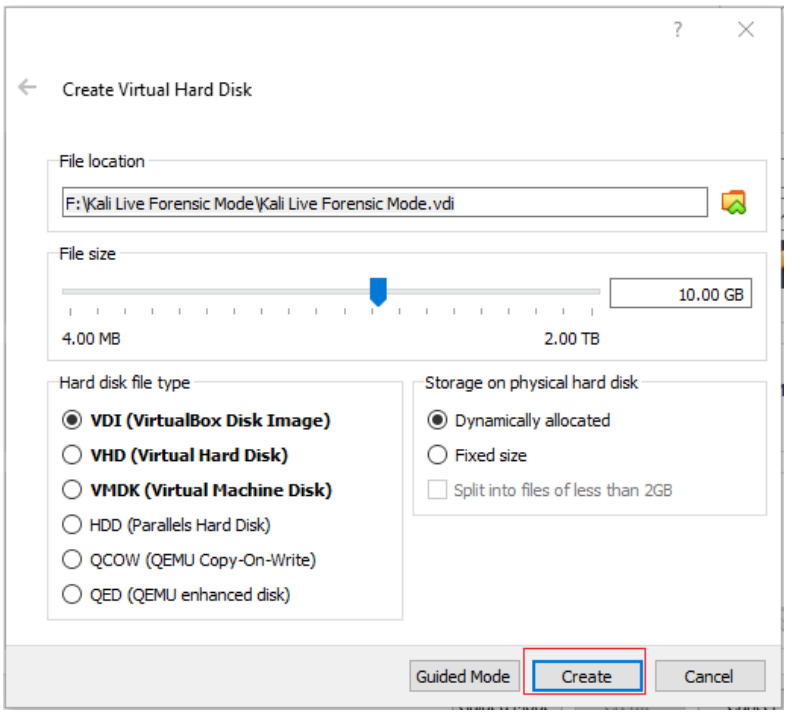
On create a virtual machine wizard launches. On the first screen, give your virtual machine a user-friendly name. In this example, I have named my VM, “Kali Live Forensic Mode.” For the Machine Folder, select a location to store the machine (recommend a separate volume or partition away from the host operating system).

- Type: ‘Linux’
- Version: Ubuntu (64-bit or 32-bit)

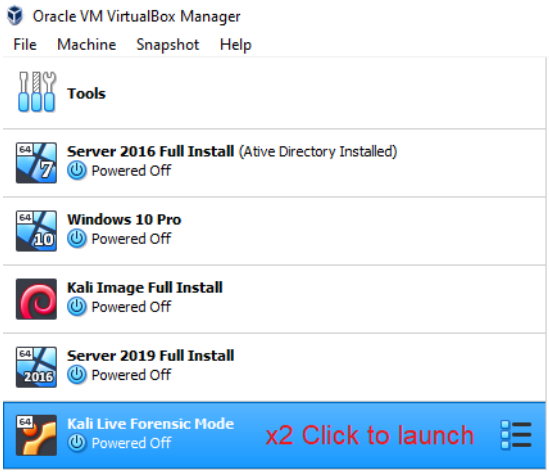
Click on, **Create**.



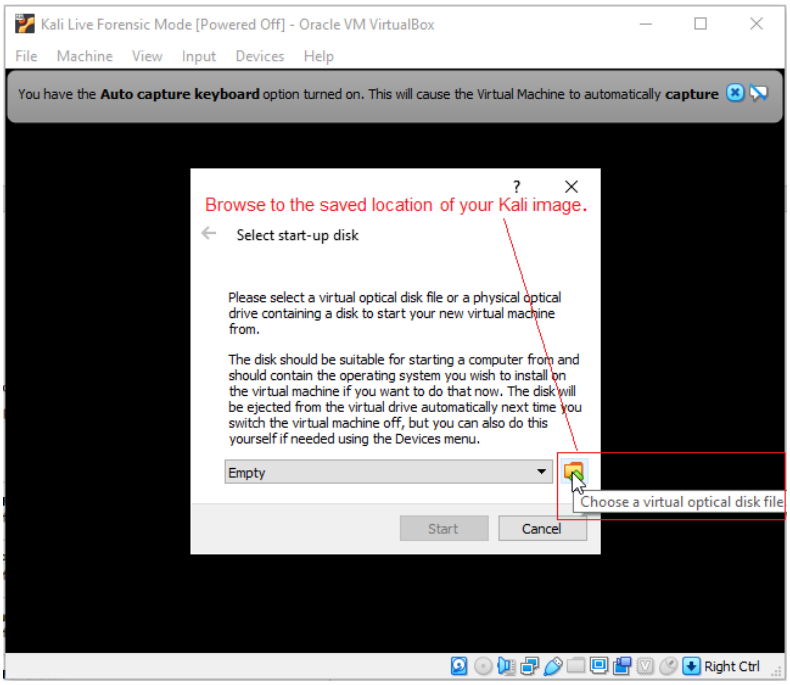
On the next screen, accept the defaults and click, **Create**.



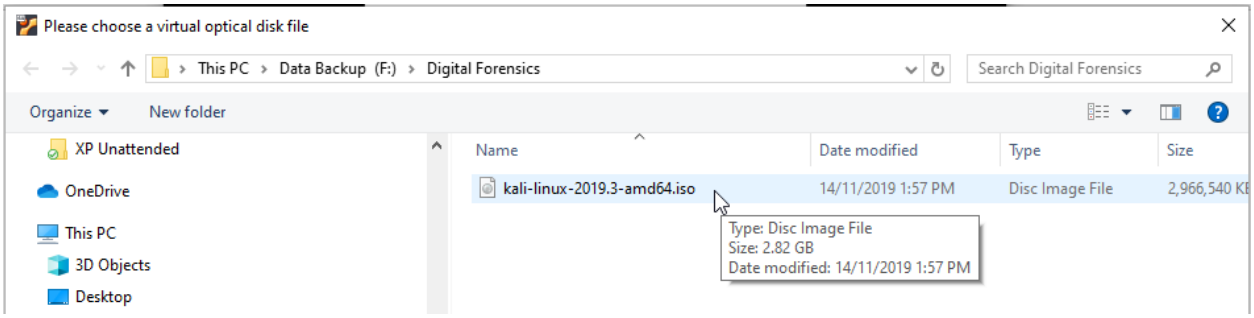
From the Left windows pane of your VirtualBox manager, x2 click on the name of your newly created virtual machine.



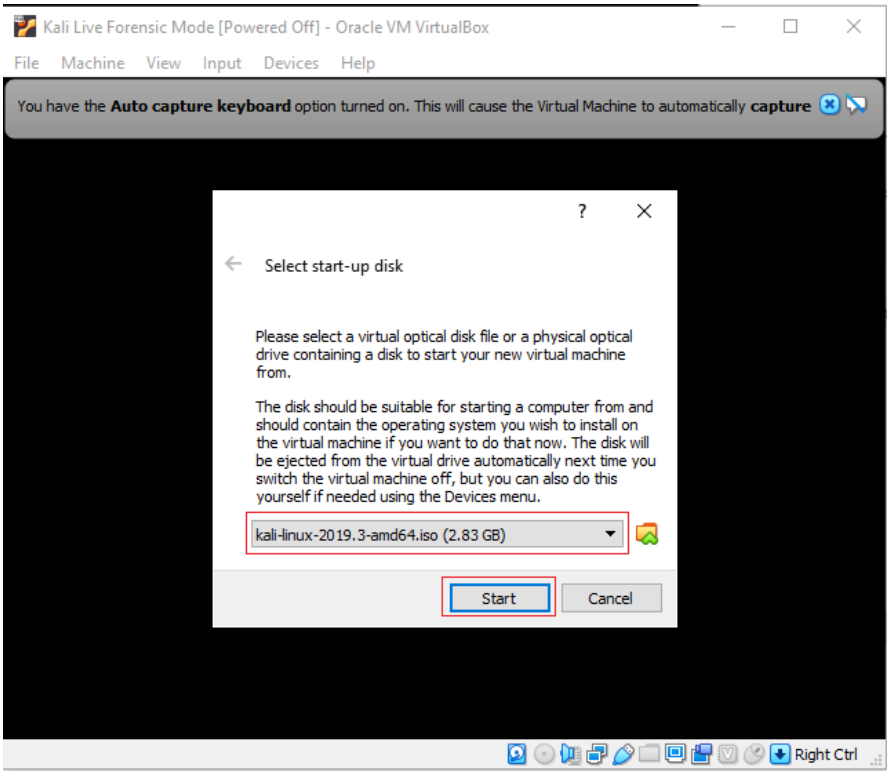
Once the machine starts, you will need to browse to the saved location of your downloaded Kali ISO image..



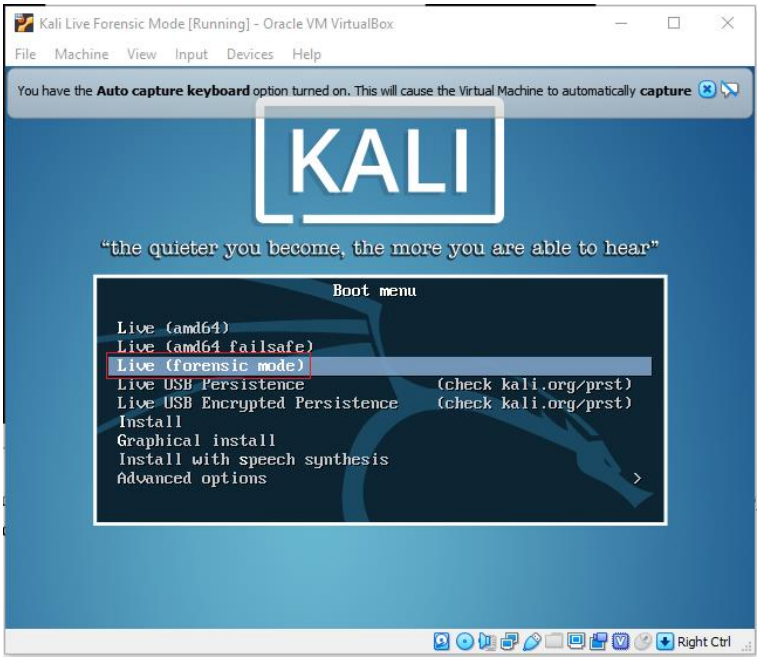
Once you find the download, x2 click the iso image to load into the window



Once you have the image loaded, click the **Start** button.



As the ISO image begins to load you, you will be given a boot menu. From the boot menu options, use your keyboard arrows to move the highlighted selection up or down until you have selected the correct option, **Live (forensic mode)**. With the correct option selected, from your keyboard, press enter to launch Kali as a live CD.



Kali begins to load. Be patient. The screen should go dark until the files have been loaded into memory. Wait for the desktop to appear.

This is the live (forensic mode) desktop.

Summary

In this lab, you learned how to use VirtualBox to create a virtual Kali Live (Forensic Mode) CD. In our next video and lab, you will learn how to add a forensic image to VirtualBox for cloning using the Kali Live (Forensic Mode) desktop.

End of the lab!