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.

In Live (Forensics Mode), the Kali operating system does not mount the suspect's hard drives. Thereby, Kali does not write or leave any metadata or changes to the suspect'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 all the files visible to the operating system and deleted files and pieces of files left in the slack and free space.

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

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

Lab Requirements:

Be sure to review the lab file before you begin

1. A download of the Kali Live Boot ISO Image from https://www.kali.org/get-kali/#kali-live
2. Install VirtualBox Latest Edition with the extension pack
3. CPU that supports Virtualization.
4. 8GB of RAM preferred. (4 GB of RAM will Suffice but is not optimal)
5. At least 60 GB of free hard drive space. (An external hard drive or thumb drive can also be used as storage)

Using Kali Live (Forensic Mode)

In this course, we will be simulating acquiring a forensic image. Different images will be provided throughout the course to gain experience using the other forensic tools and techniques presented. Usually, 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 would help if you made 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 (next lab).

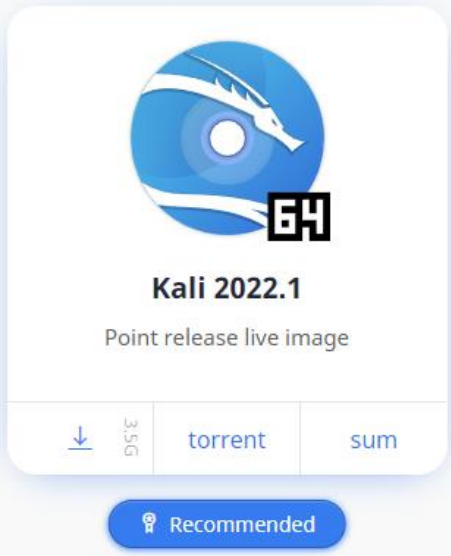
Once we have a Kali desktop, we will create a forensic image using Kali's command line or terminal software write blocker. This process will be repeated with each forensic lab as needed.

Why do 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 remove the "Kali Live" DVD or USB drive and restart the system.

Download the Kali Live 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/get-kali/#kali-live

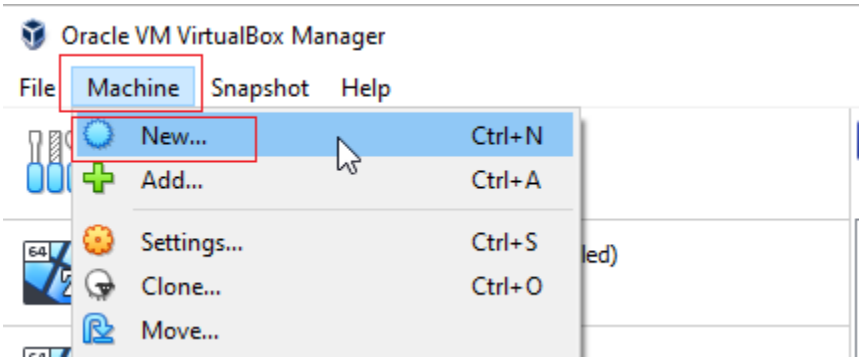


I recommend that you use the direct download and not the torrent option. The torrent option can sometimes pull in corrupted files from one of the many torrent peers.

Save the image to a location on your machine.

Launch Kali in Live Forensic Mode

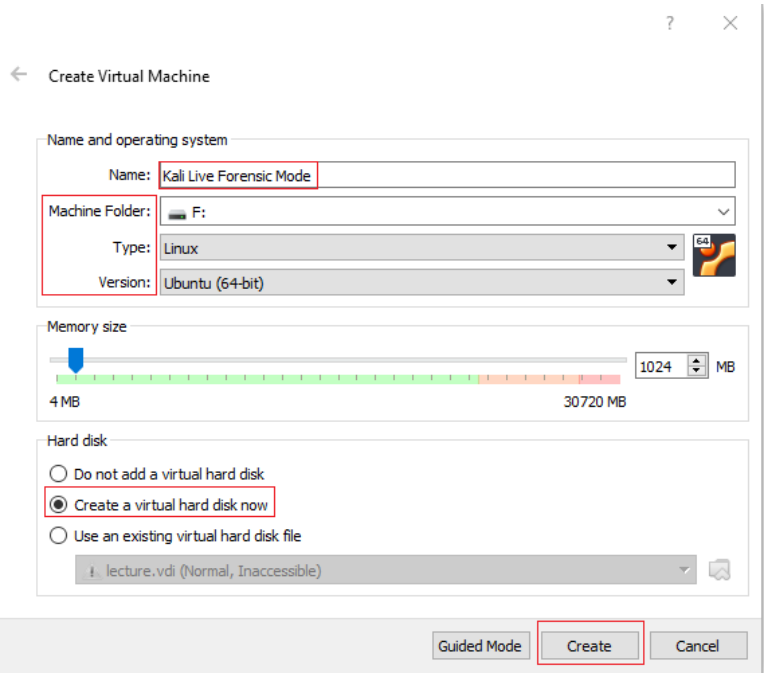
Open your install of Virtual Box Manager and from the overhead taskbar, click on **Machine,** and from the context menu, select **New**.



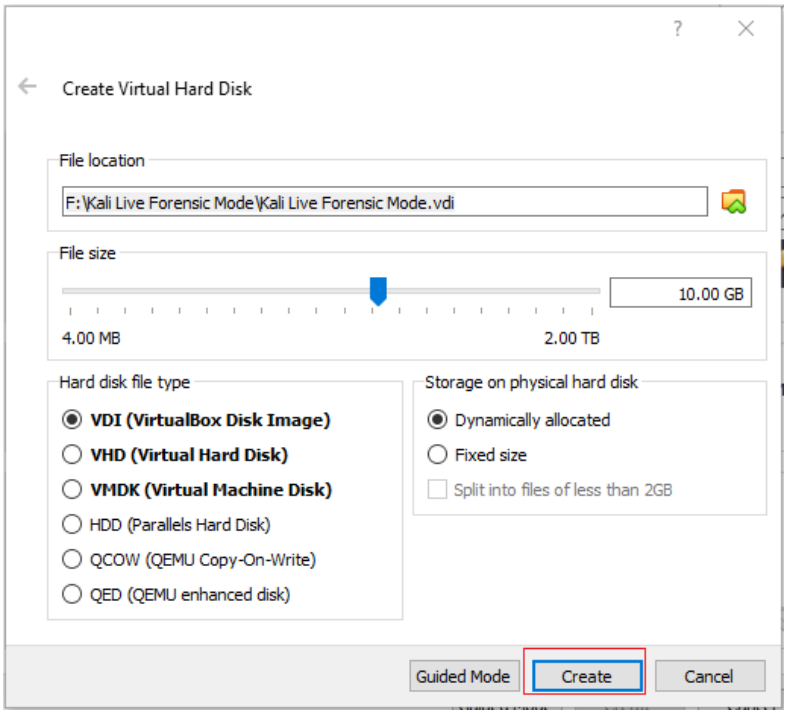
To create a virtual machine, wizard launches. On the first screen, give your virtual device a user-friendly name. In this example, I have named my VM "Kali Live Forensic Mode." Select a location to store the machine (recommend a separate volume or partition away from the host operating system).

- Type: 'Linux.'
- Version: Ubuntu (64-bit or 32-bit)

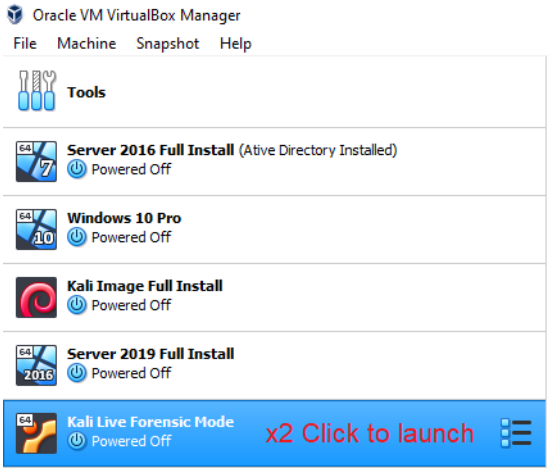
Click on, **Create**.



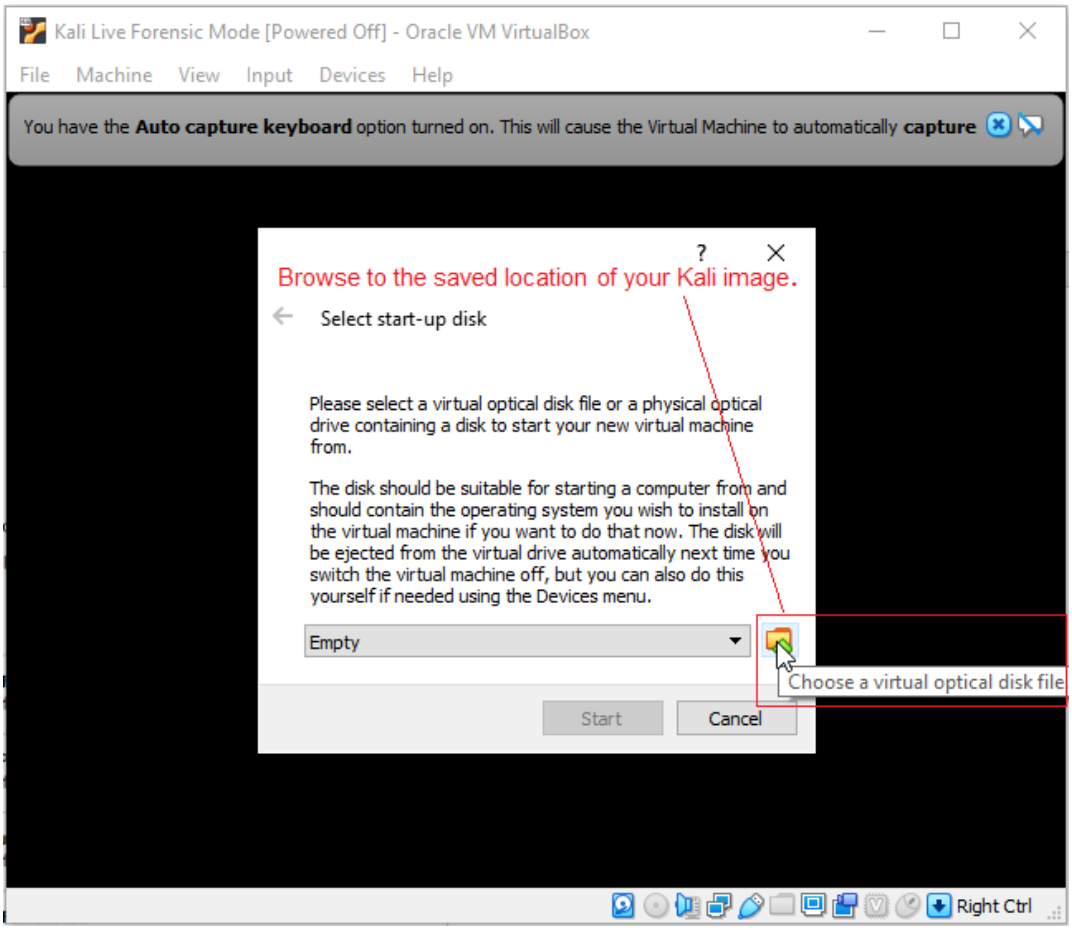
On the next screen, accept the defaults and click, **Create**.



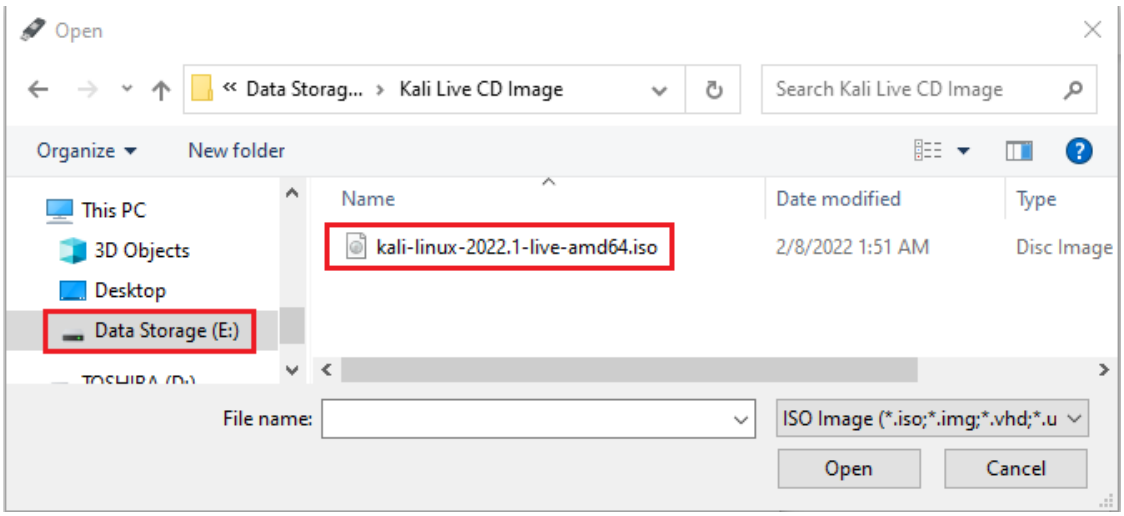
From the Left windows pane of your VirtualBox manager, x2 click on the name of your newly created virtual machine.



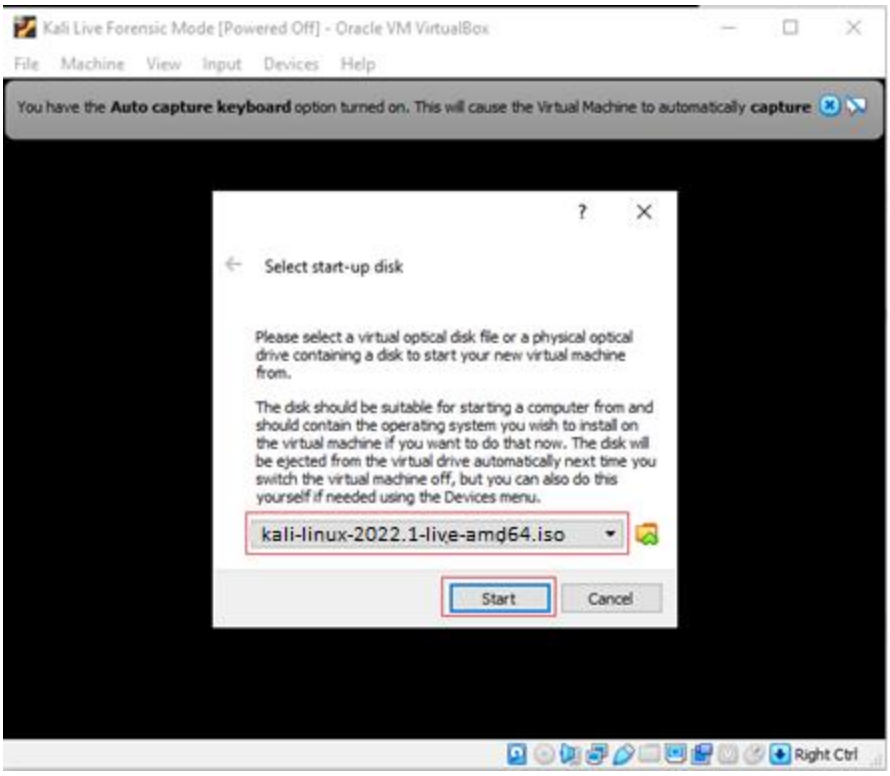
Once the machine starts, you will need to browse your downloaded Kali ISO image.



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

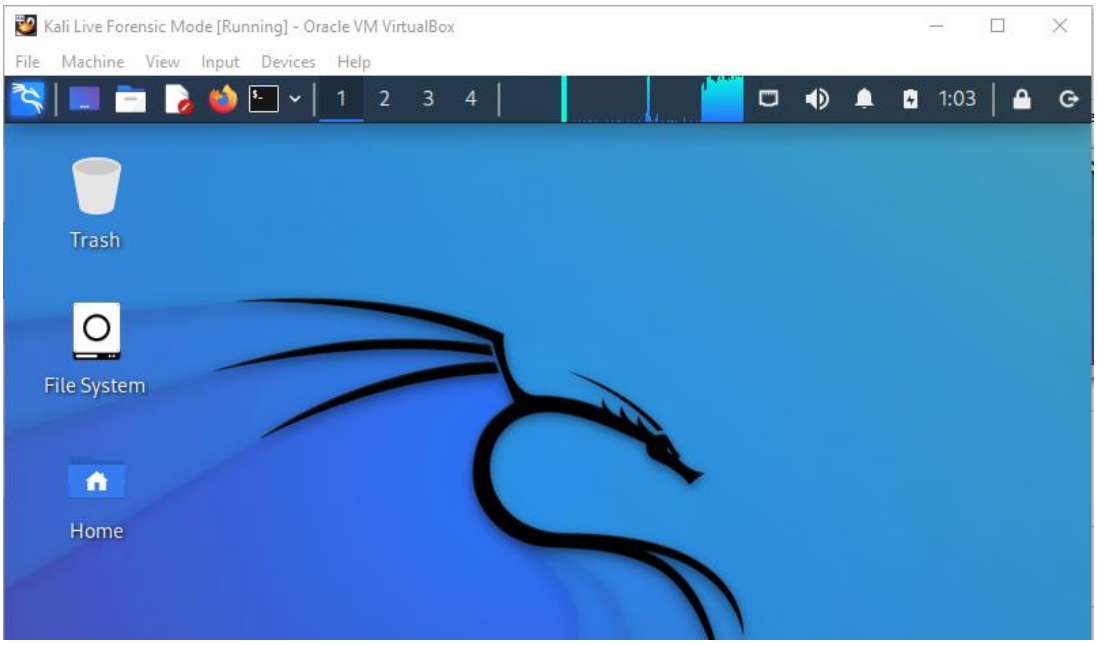


Once you have the image loaded, click the **Start** button.



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 choice, **Live (forensic mode)**. With the right option selected, press enters to launch Kali as a live CD from your keyboard.

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.

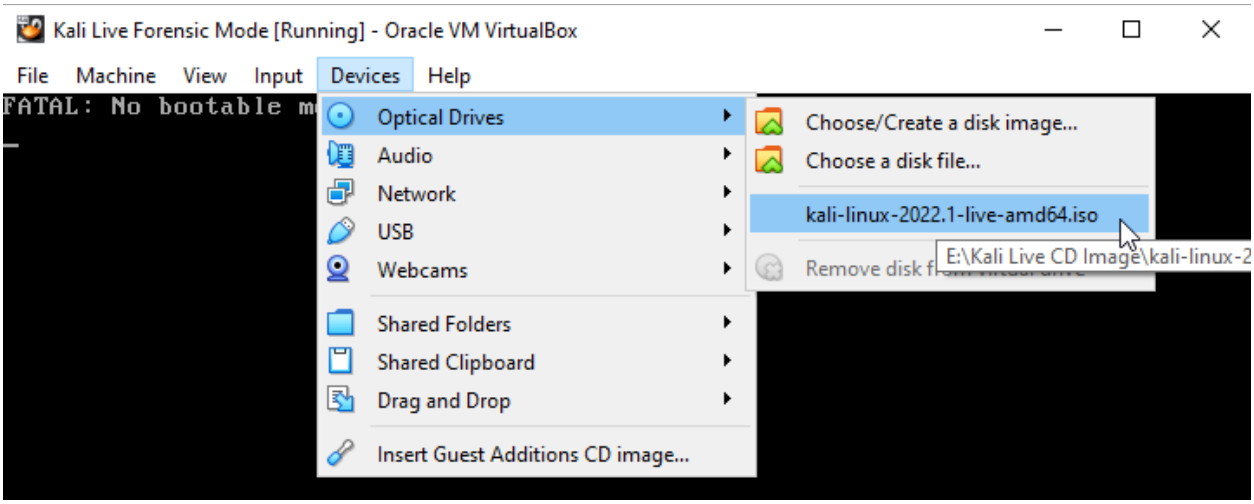


This is the live (forensic mode) desktop. Use the shutdown button to power off the machine.

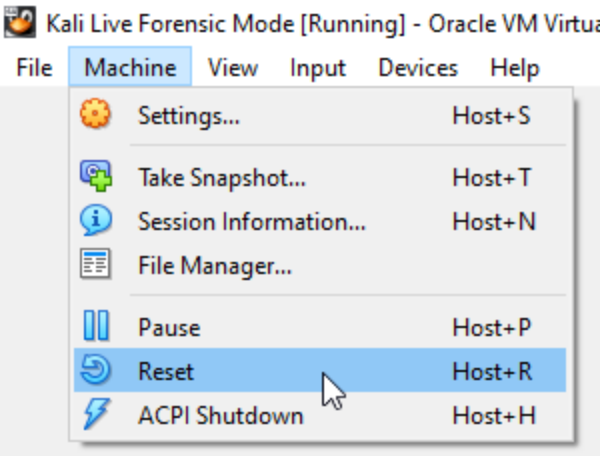
Since the Kali image is not installed, each time you launch the VM, you will have to point the disk to the location of the Kali Live ISO image.

Launch your VM of Kali forensic Mode.

Once the VM has started, click on device optical drives from the taskbar, and the context menu, select the Kali Live ISO image.



You next need to click on Machine, and from the context menu, select reset.



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 to add a forensic image to VirtualBox for cloning using the Kali Live (Forensic Mode) desktop.

End of the lab!