Lab - Create a Kali Live (Forensic Mode) Bootable USB

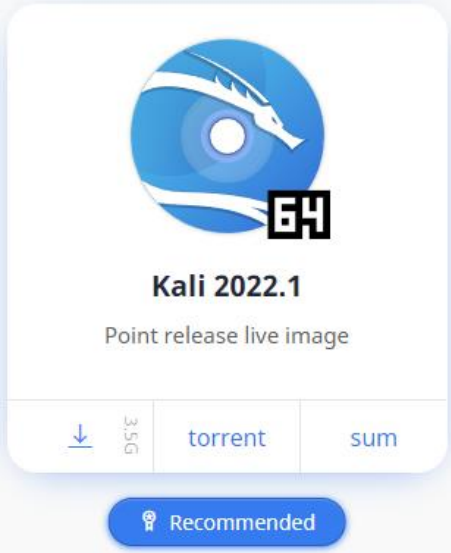
Overview

A Kali Linux Live image on USB can allow you to access a full bare metal Kali install without needing to alter an already-installed operating system. This allows for easy access to the Kali toolset with all the advantages of a bare metal install.

Booting into Kali (Forensic mode) does not mount system hard drives hence the operations you perform on the system do not leave any trace.

Lab Requirements

A download of the Kali Live Boot ISO Image from https://www.kali.org/get-kali/#kali-live



For Windows users, a download of the Rufus executable for creating a USB Kali Live Bootable Image. https://rufus.ie/en/

For Linux users, you can use the free USB flash drive utility called Etcher.

One USB flash drive that can be formatted clean. You can get away with using a 4 GB flash drive, but it is recommended a size of at least 8 GB.

Begin the lab!

For this demonstration, I will be using Rufus. I have downloaded the Kali Live Boot Image, and it is stored locally on my Windows 10 machine.

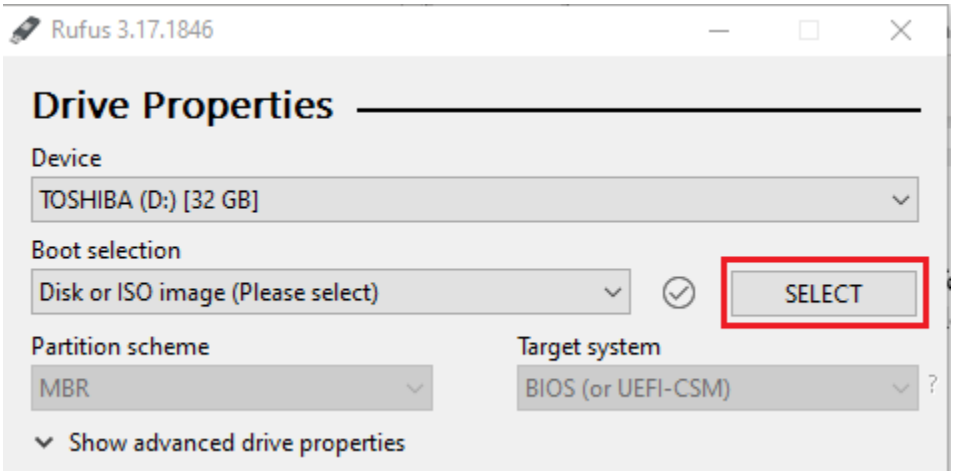
I have downloaded Rufus. It, too is saved to my local machine.

I have a 32GB USB flash drive that has nothing of importance. Rufus with format the drive deleting anything I leave on the drive. **The USB flash drive will be formatted clean.**

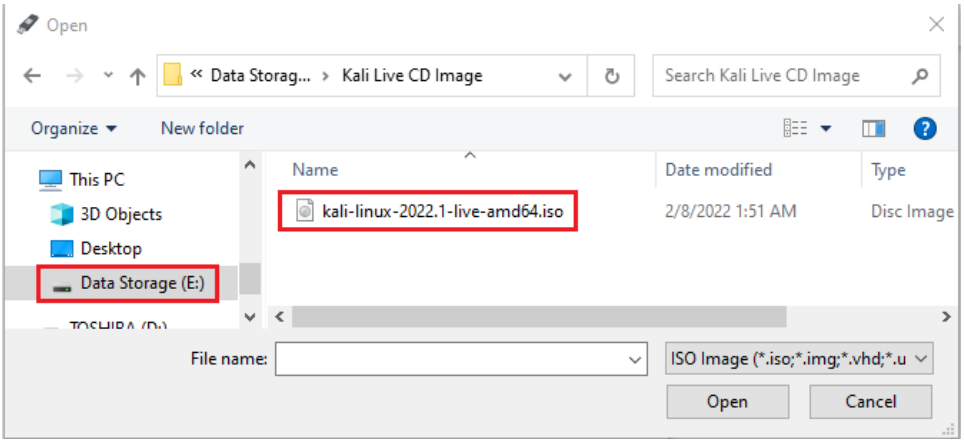
Plug the USB flash drive into any available USB port on your machine.

Rufus is a self-running executable and requires no installation. Find where you downloaded and saved Rufus and x2 click to launch the program. Rufus has identified my 32GB USB flash drive.

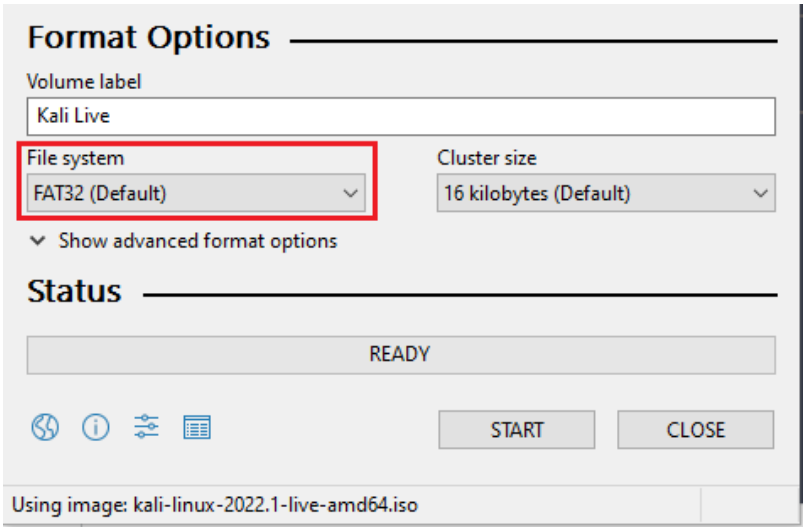
I next need to give Rufus the location of my Kali Live Boot ISO Image. I press the select button and browse to the saved location for the image.



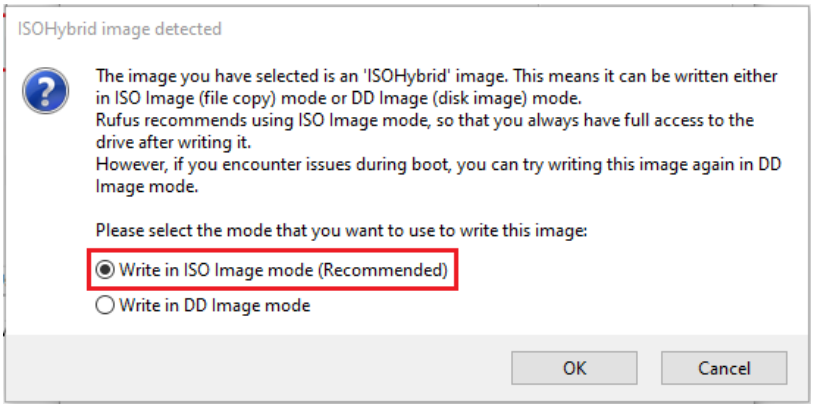
I browsed the download location where I saved the Kali Live Boot ISO Image. To load the image, I x2 click the name of the ISO image.



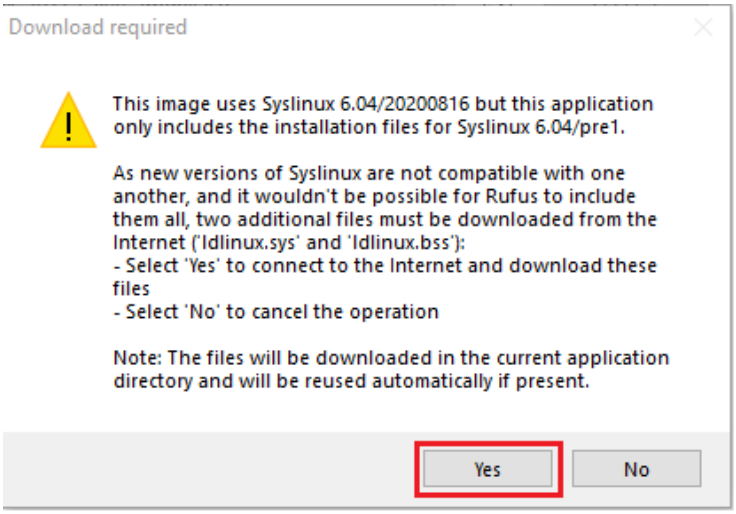
Rufus identifies the image and labels the volume as Kali Live. Rufus notes that this is a Linux image, so it formats the volume using FAT32.



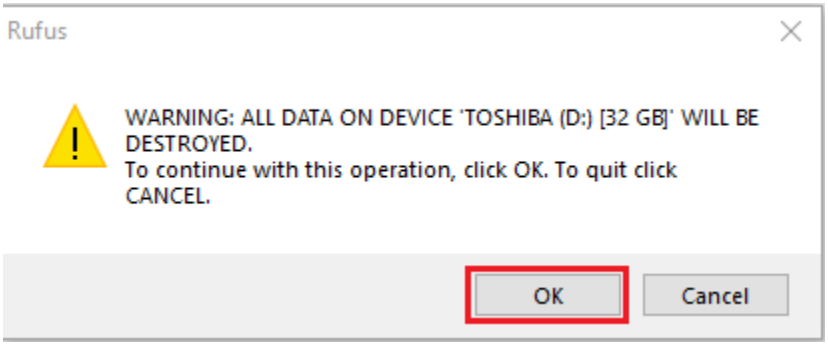
When you are ready to create your Kali Live Forensic Image, press the start button. Rufus gives you one of two options for creating the bootable image. Accept the default recommended and press the OK button.



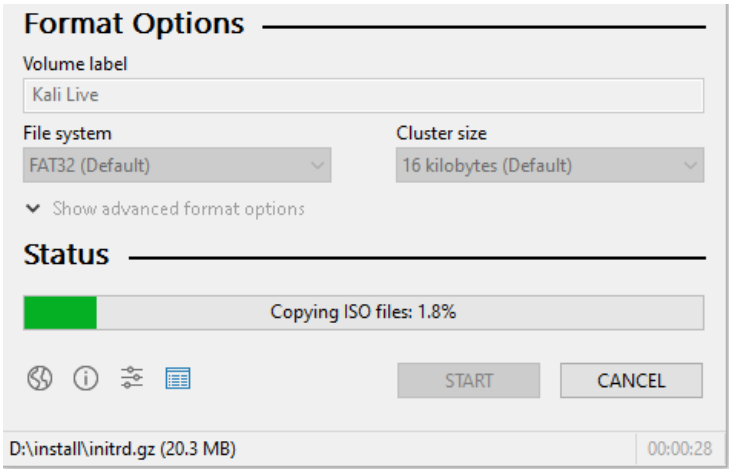
On the next screen, you may be prompted to download the version of the Syslinux needed for the build. Say yes to the download.



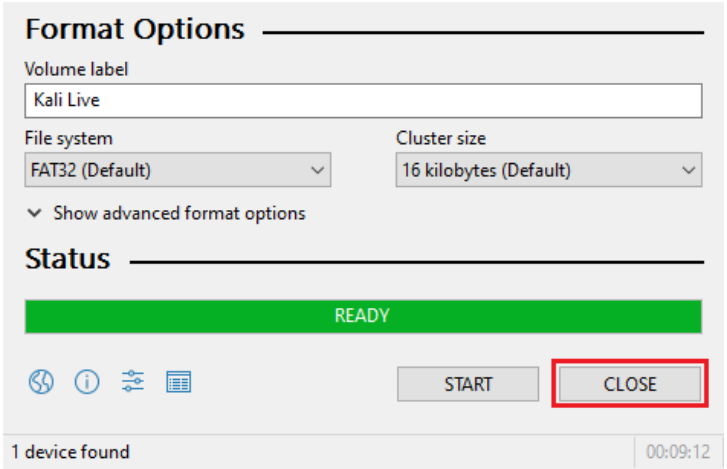
Rufus gives you one last warning about formatting and deleting anything on the USB flash drive. Press the OK button.



The build process begins. Be patient. In build process may seem as if it has stalled but it is copying over 3GB of files to the USB drive. Again, be patient!



When the build process is complete, Rufus returns to a state of readiness. You can close the application.



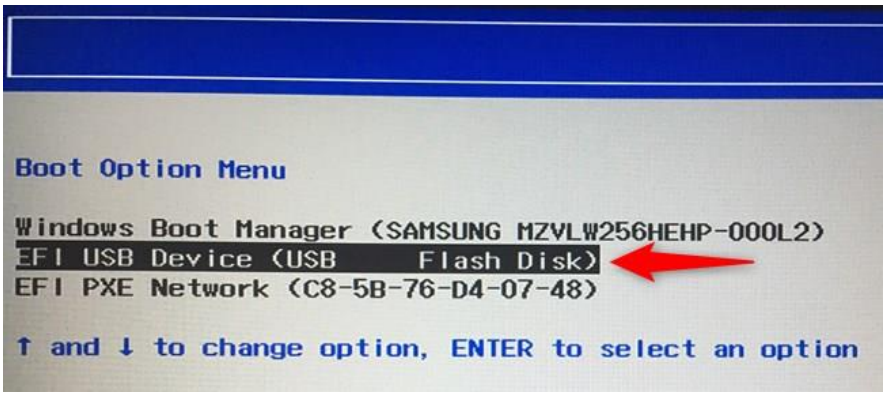
Boot from the Kali Live USB

There are several different ways to tell the system to boot using a USB flash drive. Most modern motherboard manufacturers offer a function key that can be tapped at startup to enter a boot menu. This is either the F9, F10, F11, or F12 function key. If you have an OEM machine such as a Dell or HP, you can find how to access the boot menu by going online.

To access the Boot Menu, find your PC manufacturer below to see what combination of keys you need:

- **Acer:** Esc, F12 or F9. Most computers models from Acer should work with the F12 key.
- **Asus:** F8 or Esc
- **Compaq:** Esc or F9
- **Dell:** F12
- **eMachines:** F12
- **Fujitsu:** F12
- **HP:** Esc or F9. If Esc works, you may need to press F9 afterwards: Esc + F9.
- **Lenovo:** F8, F10 or F12. On computer models with the Novo button, try pressing the Novo button. Other key combinations: Fn + F11.
- **Samsung:** Esc or F2 or F12. Users of ultrabooks from Samsung should disable the fast boot option in BIOS/UEFI before they boot from a USB device. To disable the fast boot, go to To access BIOS/UEFI > Samsung and find the combination of keys you need to press to access this.
- **VAIO:** Esc, F10 or F11. On some Sony VAIO computers models you may need to press the Assist button.
- **Toshiba:** F12

Once you have access to the boot menu, select your USB option.



Configure the BIOS to boot from a USB

If no boot menu is available, you can access the machine's BIOS and select the first boot device as the USB. Accessing the BIOS is not recommended for the faint of heart. If you do not know what you are doing, stay out.

Motherboard and OEM manufacturers use different BIOS manufacturers. With a modern BIOS, you must disable secure boot, enable legacy mode and then make your USB the first boot device in the boot order.

Choosing Which Kali Live Mode to Use

Once you've booted into the Kali Live USB flash drive, you should see a few different options for which version of Kali you want to load. They may include:

- **Live system:** This will boot up Kali Live. In this mode, you cannot save any changes. No reports, no logs, no other data — none of these changes are saved. This way, you start with a fresh Kali Live every time you boot it up. Data is only saved to RAM, not the drive.
- **Live system (fail-safe mode):** Same as the live system, but a more robust version in case the system fails. That way, the failed system won't ruin your flash drive. This is a good option if you need to troubleshoot a problematic computer.
- **Live system (forensic mode):** Same as the live system with forensic-friendly tools so that you can recover files, gather evidence and perform other forensic tasks on a host machine. However, the internal hard drive is never touched, and external devices and media will not auto-mount so that you have complete control over what you can connect to.
- **Live system (persistence):** Same as the live system, only changes will be saved, and it will allow you to inspect the host system without worrying about running or locked processes.

- **Live system (encrypted persistence):** Same as the live system (persistence), only encrypted with LUKS, so it's harder for others to access your data.
- **Start installer:** This lets you start the installer to install Kali on an internal drive.
- **Start installer with speech synthesis:** Same as start installer, only with speech instructions to help navigate.
- **Advanced options:** Includes options such as MemTest, Hardware Detection, etc.

Summary –

In this lab, you learned how to easily create a Kali Linux bootable USB device. You could do the same thing with any bootable ISO image whether it be Windows 10 or Red Hat Server.

End of the lab!

.