Lab – Simulate Creating a Disk Image for a Forensic Analysis

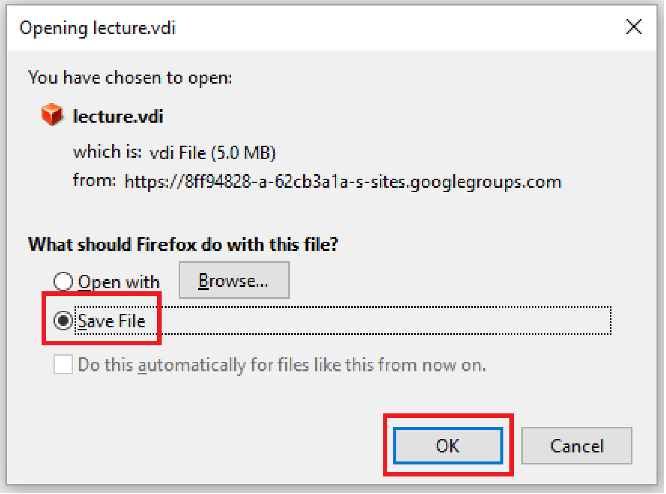
Overview

In this short lab, you will learn how to attach a disk to a SATA controller in VirtualBox that will represent a suspect's hard drive. Your will then use your Kali Live (Forensic Mode) virtual machine to acquire the disk and create a forensic copy of the disk to later be analyzed.

Download the needed image file

We first need to download the VirtualBox disk from the Internet using the following URL.

www.mikemurphy.com/forensics/lecture.vdi



Opening lecture.vdi

You have chosen to open:

lecture.vdi

which is: vdi File (5.0 MB)

from: https://8ff94828-a-62cb3a1a-s-sites.googlegroups.com

What should Firefox do with this file?

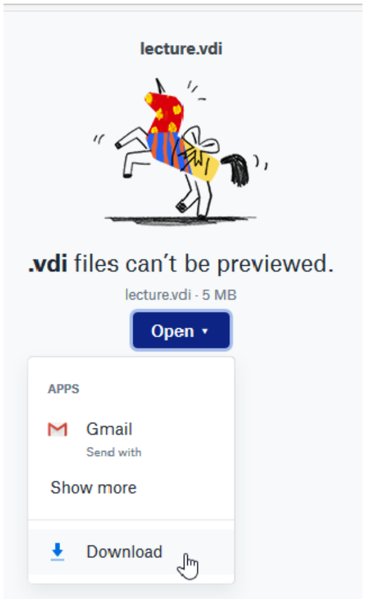
○ Open with

● Save File

□ Do this automatically for files like this from now on.

The following location is available in the event the download location for the VDI is no longer available

Backup location for the Lecture.vdi Click on the open link and from the content menu, select download.



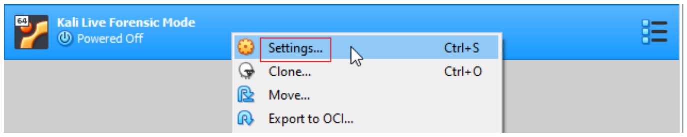
lecture.vdi

.vdi files can't be previewed.

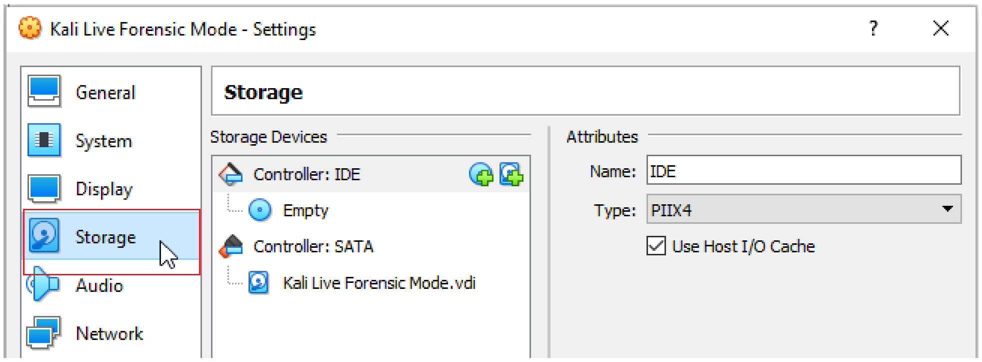
lecture.vdi · 5 MB

Launch your installation of VirtualBox

From the left-hand window pane of your VirtualBox manager, right click on the name of your Kali Live (forensic Mode) virtual machine and from the context menu, select **settings**.



From the left windows pane of your settings menu, click on **Storage**.

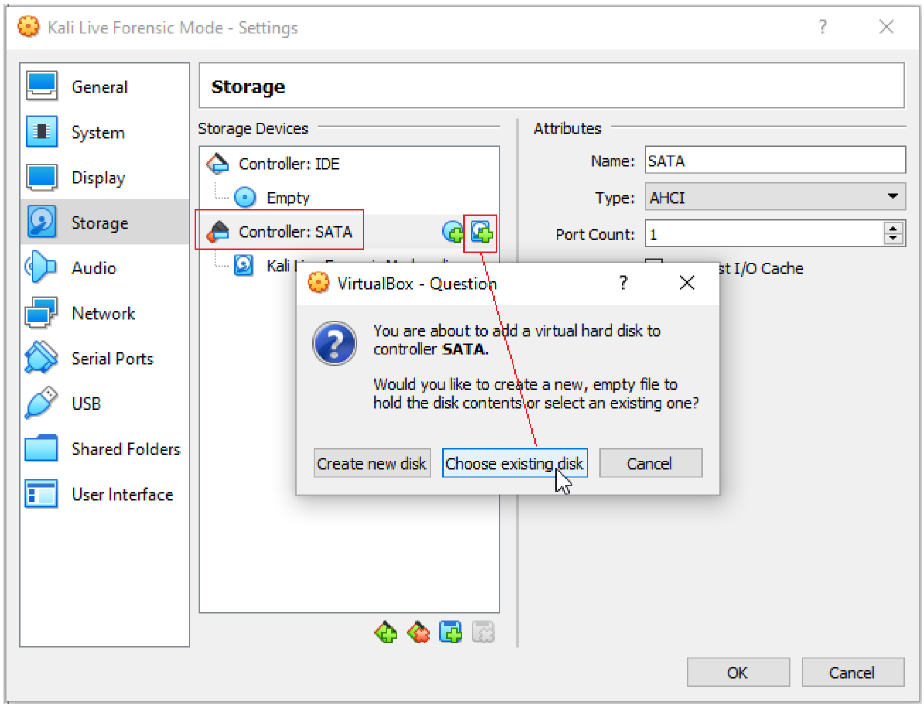


Name: IDE

Type: PIIX4

☑ Use Host I/O Cache

Under storage Devices, highlight your **Controller: SATA** controlling your Kali Live (Forensic Mode) VDI and then click on the plus (+) icon to add a hard disk. From the pop-up window, click on the **Choose existing disk**.



Name: SATA

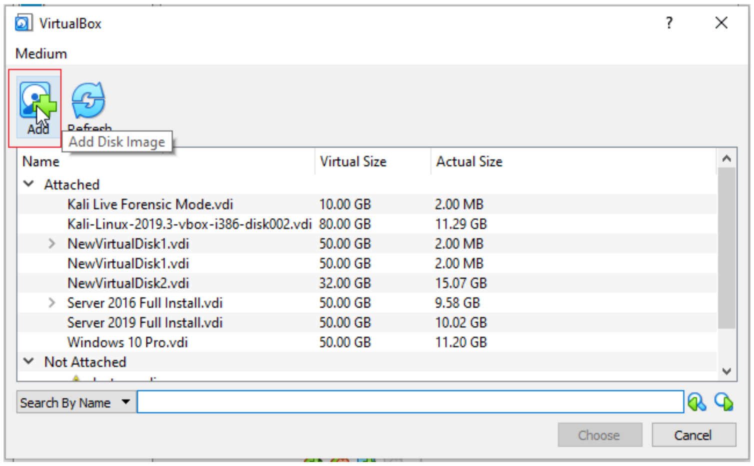
Type: AHCI

Port Count: 1

You are about to add a virtual hard disk to controller **SATA**.

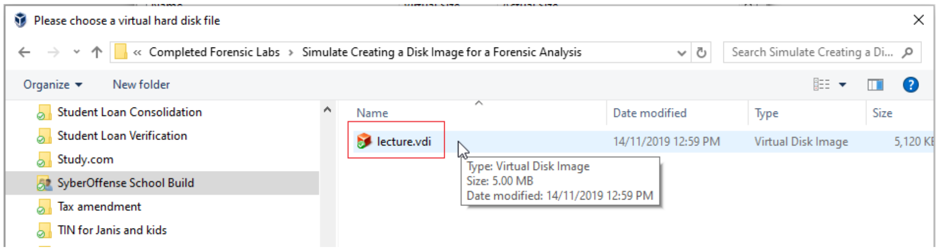
Would you like to create a new, empty file to hold the disk contents or select an existing one?

On the next screen, click on the plus (+) icon to browse and attach the lecture.vdi image previously downloaded.



Name	Virtual Size	Actual Size
Attached		
Kali Live Forensic Mode.vdi	10.00 GB	2.00 MB
Kali-Linux-2019.3-vbox-i386-disk002.vdi	80.00 GB	11.29 GB
NewVirtualDisk1.vdi	50.00 GB	2.00 MB
NewVirtualDisk1.vdi	50.00 GB	2.00 MB
NewVirtualDisk2.vdi	32.00 GB	15.07 GB
Server 2016 Full Install.vdi	50.00 GB	9.58 GB
Server 2019 Full Install.vdi	50.00 GB	10.02 GB
Windows 10 Pro.vdi	50.00 GB	11.20 GB
Not Attached		

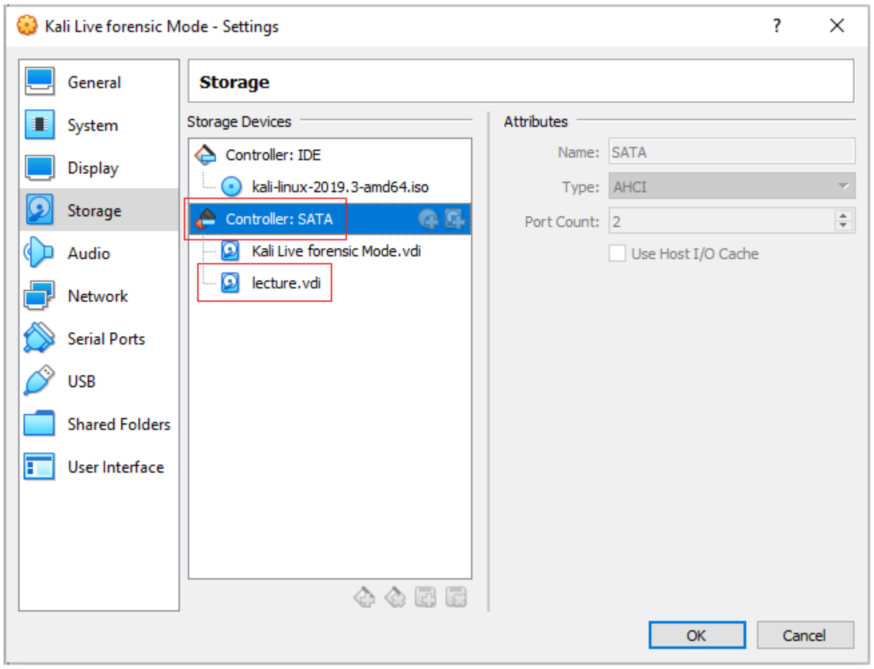
Use the next window to browse to the save location for the downloaded lecture.vdi file. Once you find the file. Just x2 click it to finish the wizard.


Please choose a virtual hard disk file
« Completed Forensic Labs › Simulate Creating a Disk Image for a Forensic Analysis
Search Simulate Creating a Di...
Organize
New folder
Student Loan Consolidation
Student Loan Verification
Study.com
SyberOffense School Build
Tax amendment
TIN for Janis and kids

Name	Date modified	Type	Size
lecture.vdi	14/11/2019 12:59 PM	Virtual Disk Image	5,120 KB

Type: Virtual Disk Image
Size: 5.00 MB
Date modified: 14/11/2019 12:59 PM

Note that the lecture.vdi is now attached to the same SATA controller as the Kali Live (Forensic Mode) vdi. This is the equivalent of attaching the image as a new disk to a physical computer.

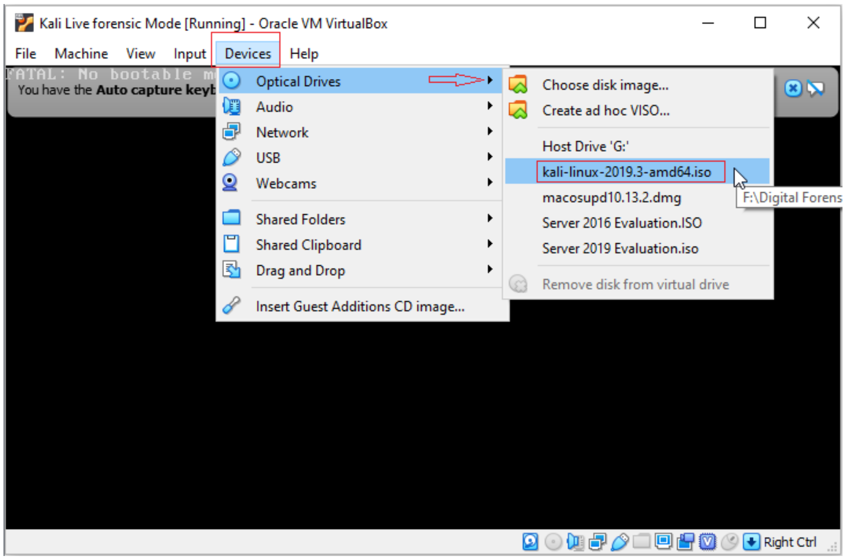


Controller: IDE
kali-linux-2019.3-amd64.iso
Controller: SATA
Kali Live forensic Mode.vdi
lecture.vdi

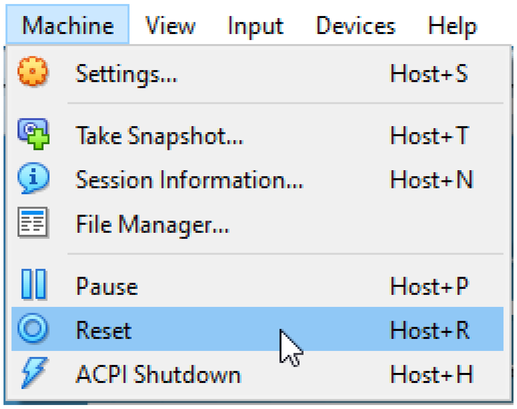
Name: SATA
Type: AHCI
Port Count: 2
□ Use Host I/O Cache

Launch your Kali Live (Forensic Mode) Virtual Machine

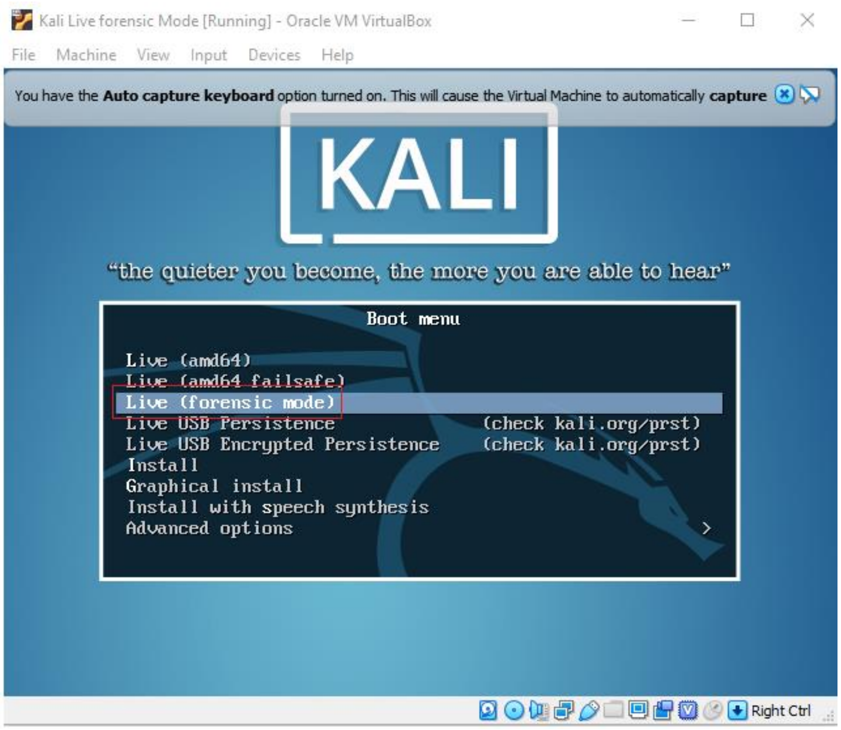
From the Left windowpane of your VirtualBox manager, launch your Kali Live virtual machine. If the Kali ISO image is no longer present in your VirtualBox CD/DVD drive, from the taskbar, click on devices, optical drives and select the name of your Kali ISO image.



Next, click on Machine and from the context menu, click on reset.



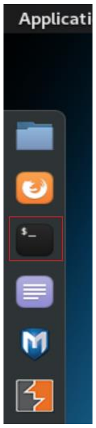
When the virtual machine rests, you will be present with the Kali boot menu. From the list of options, select Live (Forensic Mode)



You have the **Auto capture keyboard** option turned on. This will cause the Virtual Machine to automatically **capture**

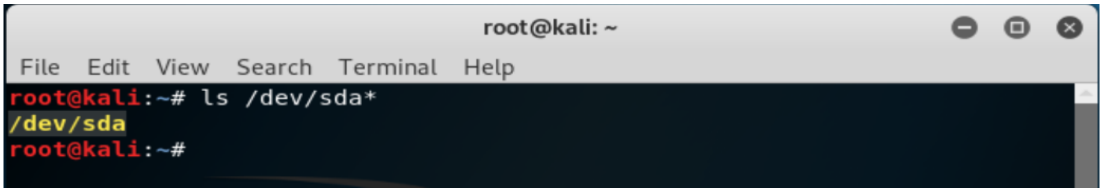
Kali Live forensic Mode [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
"the quieter you become, the more you are able to hear"
Boot menu
Live (amd64)
Live (amd64 failsafe)
Live (forensic mode)
Live USB Persistence (check kali.org/prst)
Live USB Encrypted Persistence (check kali.org/prst)
Install
Graphical install
Install with speech synthesis
Advanced options
Right Ctrl

Allow the machine to boot to the desktop. Once the machine boots to the desktop, open a terminal window.



In Linux, to look at all the hard drives that are attached to the system or to see which hard drives are attached to the SATA controller we can use the following command.

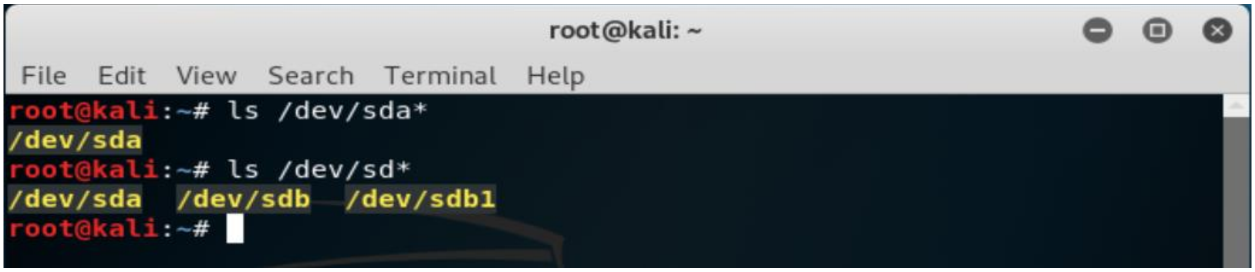
```
ls /dev/sda*
```



```
root@kali:~# ls /dev/sda*
/dev/sda
root@kali:~#
```

To see all the hard drives that are attached, we can use the following command.

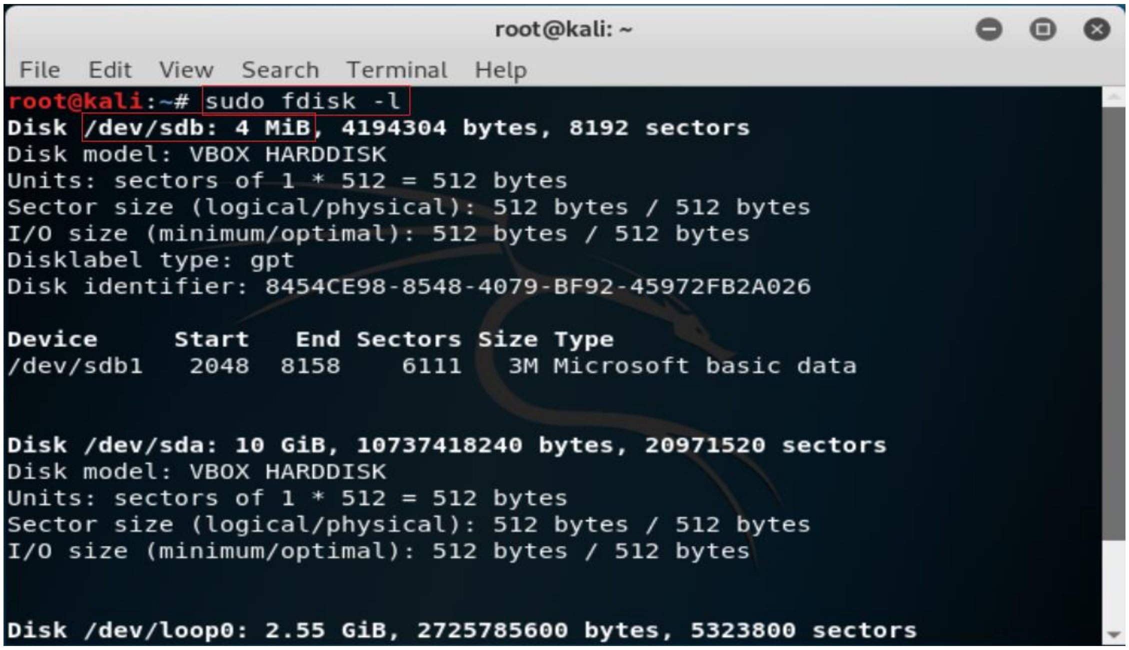
```
ls /dev/sd*
```



```
root@kali:~# ls /dev/sda*
/dev/sda
root@kali:~# ls /dev/sd*
/dev/sda  /dev/sdb  /dev/sdb1
root@kali:~# 
```

Our target disk to image is the /dev/sdb and we can confirm this by using the fdisk command to check the partitions of the drives attached to our SATA controller.

At the terminal prompt, type: `sudo fdisk -l`



```
root@kali:~# sudo fdisk -l
Disk /dev/sdb: 4 MiB, 4194304 bytes, 8192 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: 8454CE98-8548-4079-BF92-45972FB2A026

Device      Start   End Sectors Size Type
/dev/sdb1    2048  8158    6111   3M Microsoft basic data


Disk /dev/sda: 10 GiB, 10737418240 bytes, 20971520 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/loop0: 2.55 GiB, 2725785600 bytes, 5323800 sectors
```

We are currently working at the root of our Kali Live desktop. Unless we tell Kali different, anything we save will be saved to the root of our Kali machine.

We need to create a low-level forensic image using the dd command line utility.

dd is a command-line utility for Unix and Unix-like operating systems, the primary purpose of which is to convert and copy files.

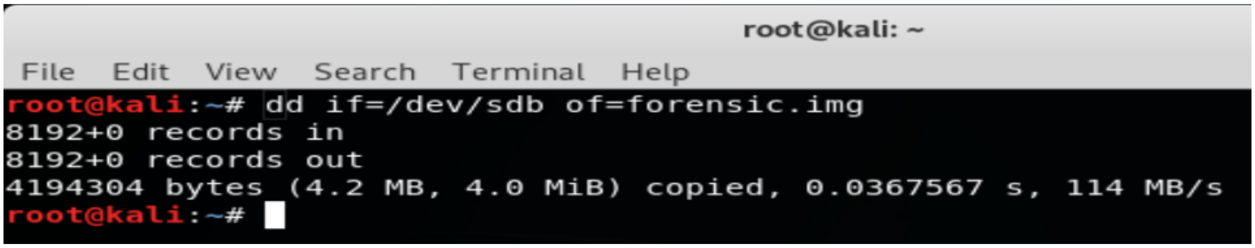
At the terminal prompt I type the following command. The drive identified as sdb is my attached drive of just under 5 MB.

```
dd if=/dev/sdb of=forensic.img
```

if stands for **input file**

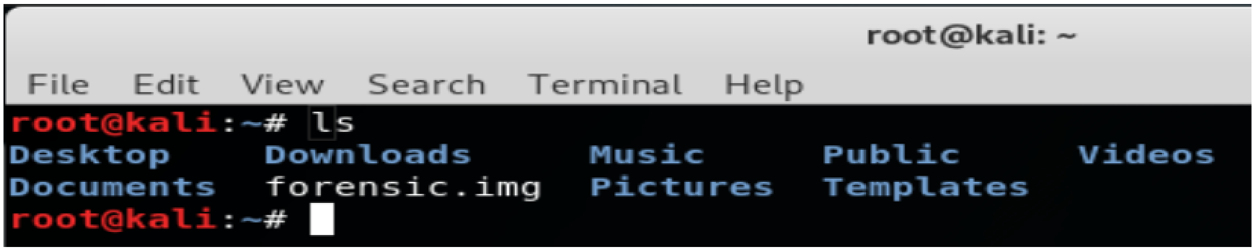
of stands for **output file**.

forensic.img is the name we have given to the output file. Since the forensic image is so small, once we hit enter, the results come right back to the prompt.



```
root@kali:~# dd if=/dev/sdb of=forensic.img
8192+0 records in
8192+0 records out
4194304 bytes (4.2 MB, 4.0 MiB) copied, 0.0367567 s, 114 MB/s
root@kali:~# 
```

Since we are doing everything from within the root directory, our forensic image file is automatically saved to the same location. To see the forensic image we created and saved to the root directory, at the terminal prompt type, **ls**.



```
root@kali:~# ls
Desktop     Downloads     Music     Public     Videos
Documents   forensic.img  Pictures  Templates
root@kali:~# 
```

Everything in blue is a directory. Our forensic.img is a file so it is shown using a white font. We created this file in memory so if we shut or reboot our Kali Forensic Mode virtual machine, we must recreate the image again using the same dd command.

Summary

We cannot save the forensic image to any location inside of out Kali Forensic Mode machine. As it is, the forensic image is stored in virtual memory so when we power down the live CD, everything will be lost. Ina real-world situation, we would have saved the output file to an external drive. In the real world where we have seized a suspect’s hard drive, we would prefer to make the forensic image back at the lab where we have the tools and storage available. A seized hard drive of 2 or 3 TBs could take days or even weeks to image.

In our next lab, we will use Autopsy to examine the forensic image we have made. If you lose the image while powering down the Kali Forensic Mode machine, you can quickly create another using the same dd command.

End of the lab!