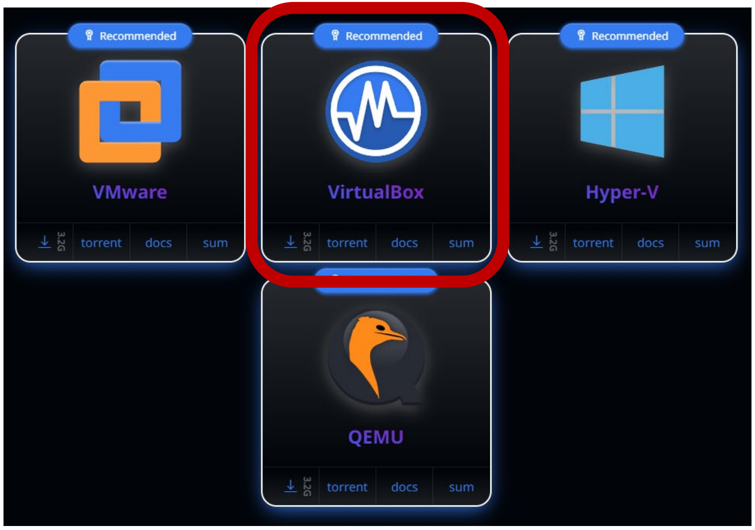
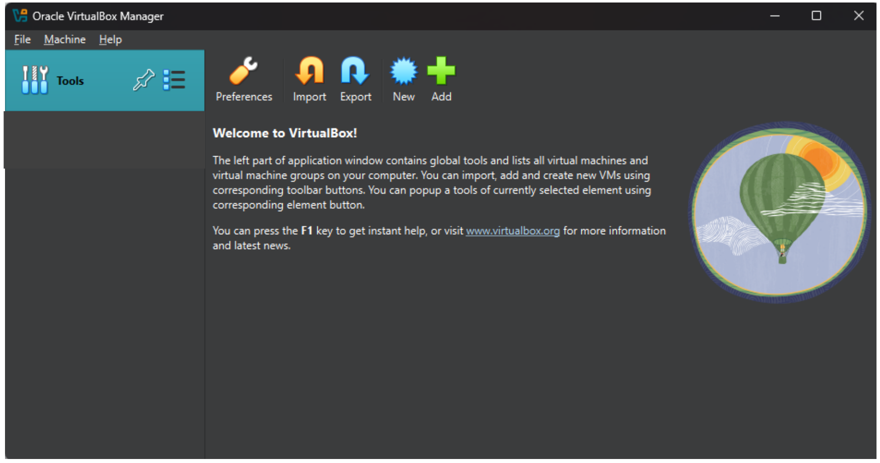
CySER Workshop – Digital Forensics
Software Install Instructions
May 2025

Software:
Memory forensic tools can be loaded on any version of a Linux OS. You will need to install a virtual machine (VM) on your computer if you don't already have one installed. I recommend VirtualBox with Kali Linux as the OS. I recommend Kali Linux because it gives you access to pre-installed cyber security analysis tools. The instructions here are specific to setting up VirtualBox with Kali Linux.

1. Install VirtualBox. The install file can be downloaded at https://www.oracle.com/virtualization/technologies/vm/downloads/virtualbox-downloads.html
2. Install Kali Linux on VirtualBox, download the Kali Linux image at https://www.kali.org/get-kali/#kali-virtual-machines using the VirtualBox image.
    a. Download the VirtualBox pre-configured image. Remember where you download this to.



    b. In your file directory, navigate to the folder you downloaded the VirtualBox image to. Unzip the 'kali-linux-2025.1c-virtualbox-amd64' folder.
    c. Open the VirtualBox manager. It should look like this after it has been installed (see step 1).

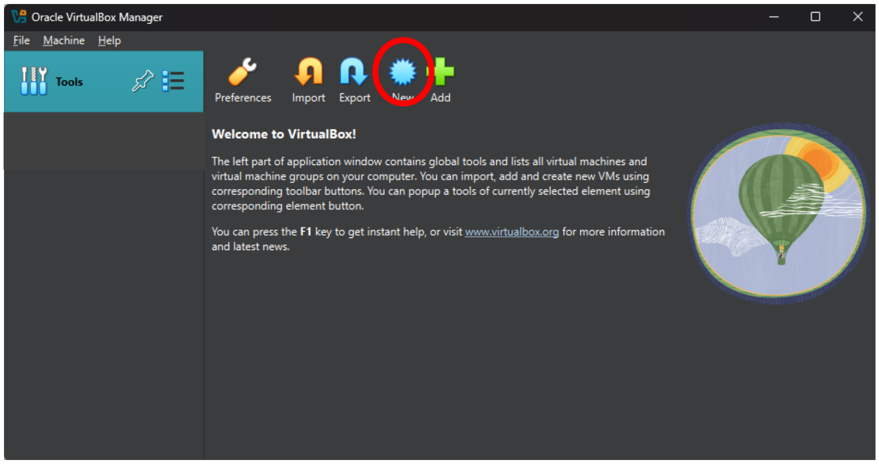


Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

    d. Click on New

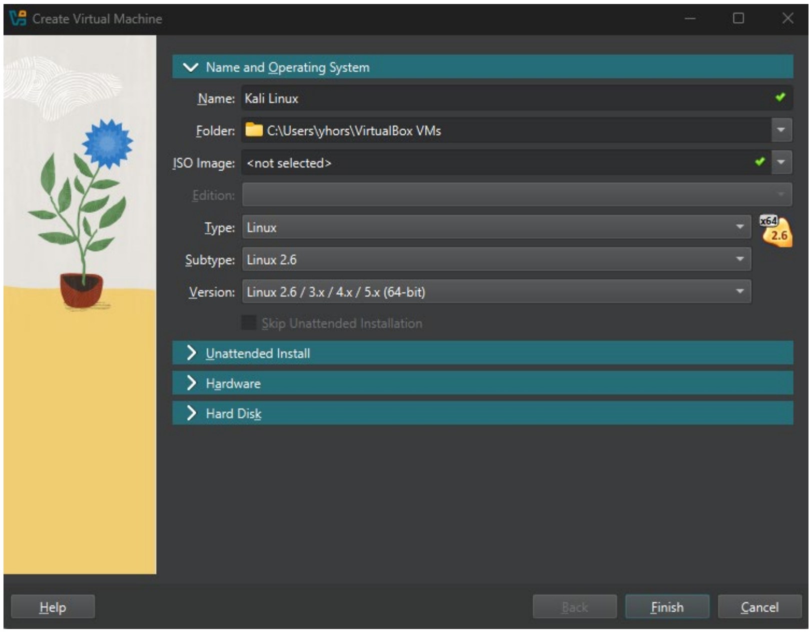


Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

e. In the Name and Operating System field, give your VM any name. I've called it 'Kali Linux'.



Name: Kali Linux

Folder: C:\Users\yhors\VirtualBox VMs

ISO Image: <not selected>

Edition:

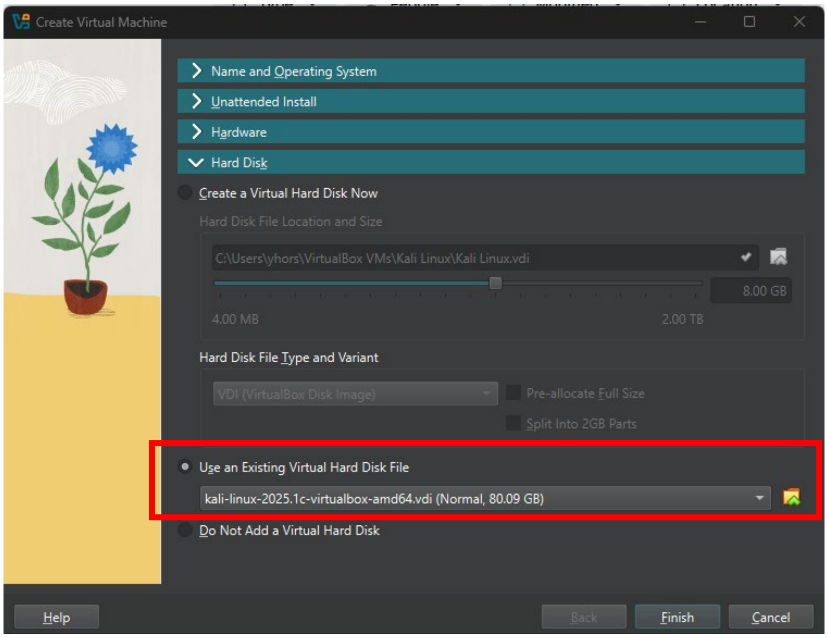
Type: Linux

Subtype: Linux 2.6

Version: Linux 2.6 / 3.x / 4.x / 5.x (64-bit)

□ Skip Unattended Installation

f. In the Hard Disk field, select 'Use an Existing Virtual Hard Disk File'. Click on the file icon to the right of this field.



○ Create a Virtual Hard Disk Now

Hard Disk File Location and Size

C:\Users\yhors\VirtualBox VMs\Kali Linux\Kali Linux.vdi

8.00 GB

4.00 MB 2.00 TB

Hard Disk File Type and Variant

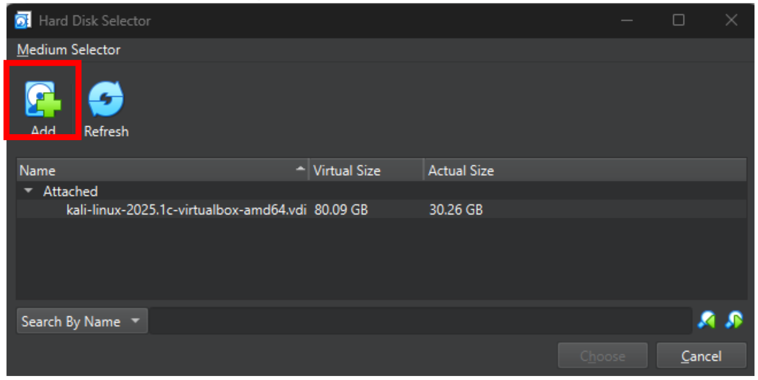
VDI (VirtualBox Disk Image) □ Pre-allocate Full Size □ Split Into 2GB Parts

● Use an Existing Virtual Hard Disk File

kali-linux-2025.1c-virtualbox-amd64.vdi (Normal, 80.09 GB)

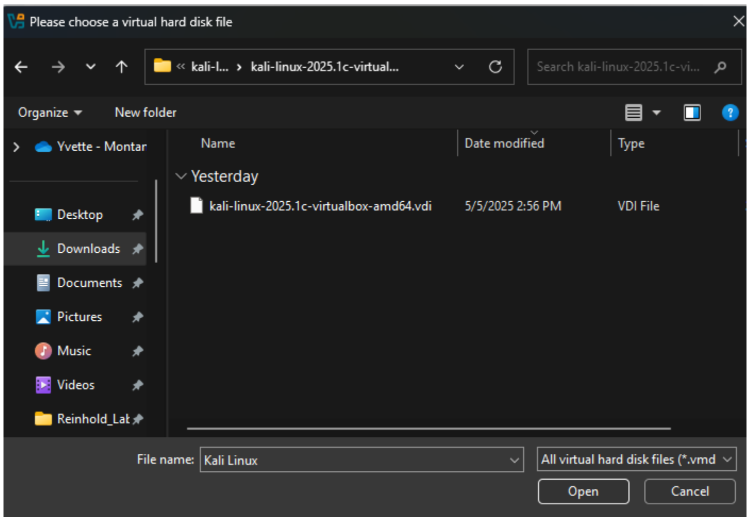
○ Do Not Add a Virtual Hard Disk

g. In the window that open's, select Add.



Name	Virtual Size	Actual Size
Attached		
kali-linux-2025.1c-virtualbox-amd64.vdi	80.09 GB	30.26 GB

h. Navigate to the folder where you have unzipped the VirtualBox image and open it. Select the 'kali-linux-2025.1c-virutalbox-amd64.vdi' file and select open.

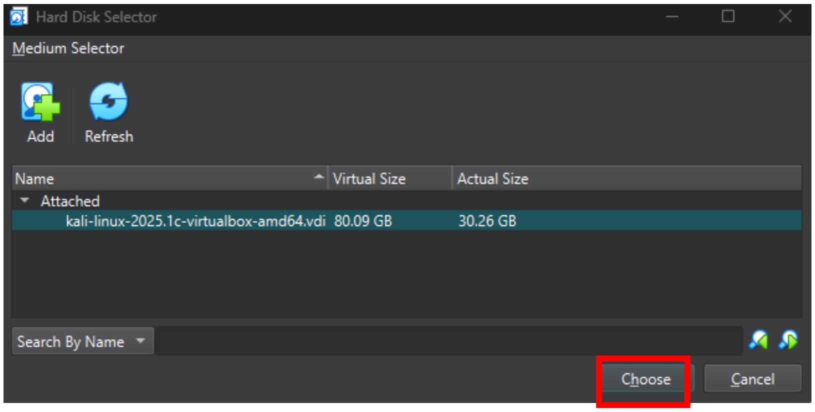

Please choose a virtual hard disk file
« kali-l... › kali-linux-2025.1c-virtual...
Search kali-linux-2025.1c-vi...
Organize
New folder
Yvette - Montar
Desktop
Downloads
Documents
Pictures
Music
Videos
Reinhold_Lat
Open
Cancel

Name	Date modified	Type
Yesterday		
kali-linux-2025.1c-virtualbox-amd64.vdi	5/5/2025 2:56 PM	VDI File

File name: Kali Linux

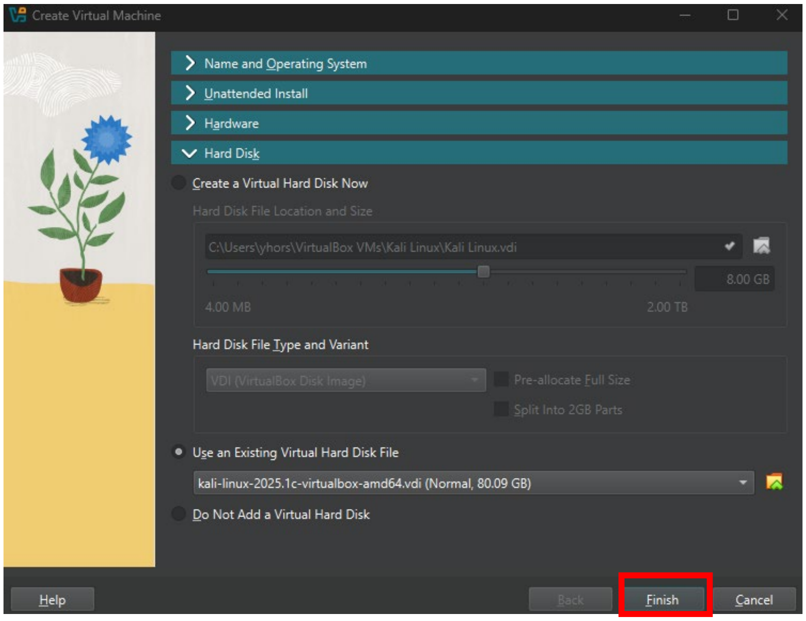
All virtual hard disk files (*.vmd

i. Click on Choose.



Name	Virtual Size	Actual Size
Attached		
kali-linux-2025.1c-virtualbox-amd64.vdi	80.09 GB	30.26 GB

j. Click on Finish.



○ Create a Virtual Hard Disk Now

Hard Disk File Location and Size

C:\Users\yhors\VirtualBox VMs\Kali Linux\Kali Linux.vdi

8.00 GB

4.00 MB 2.00 TB

Hard Disk File Type and Variant

VDI (VirtualBox Disk Image) □ Pre-allocate Full Size

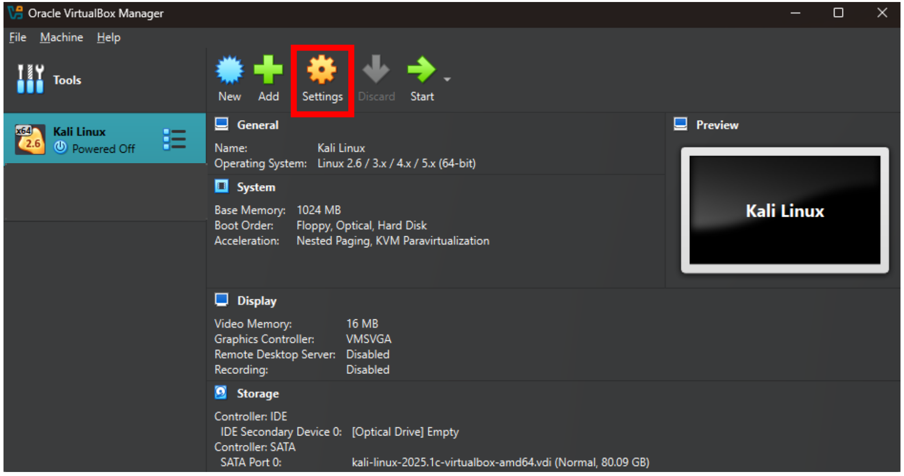
□ Split Into 2GB Parts

● Use an Existing Virtual Hard Disk File

kali-linux-2025.1c-virtualbox-amd64.vdi (Normal, 80.09 GB)

○ Do Not Add a Virtual Hard Disk

k. In the VirtualBox Manager, you will see your VM listed in the left navigation panel. With it selected, click on the Settings option.



General

Name: Kali Linux
Operating System: Linux 2.6 / 3.x / 4.x / 5.x (64-bit)

System

Base Memory: 1024 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization

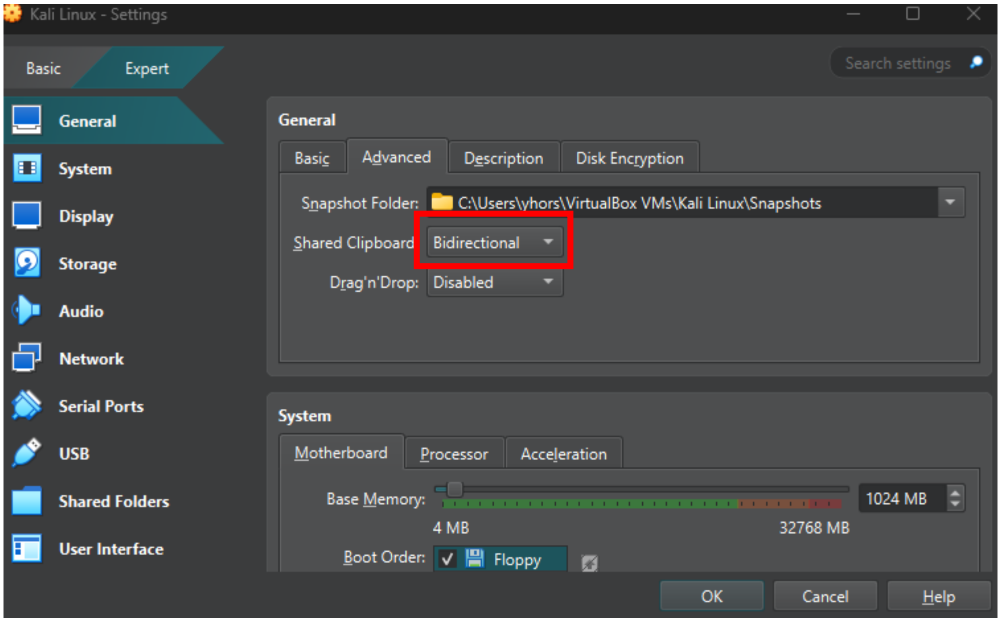
Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: kali-linux-2025.1c-virtualbox-amd64.vdi (Normal, 80.09 GB)

l. In the General box in the Advanced tab, set the Shared Clipboard to Bidirectional to allow you to copy and paste text from your computer to the VM, and vice versa.



General

Snapshot Folder: C:\Users\yhors\VirtualBox VMs\Kali Linux\Snapshots

Shared Clipboard: Bidirectional

Drag'n'Drop: Disabled

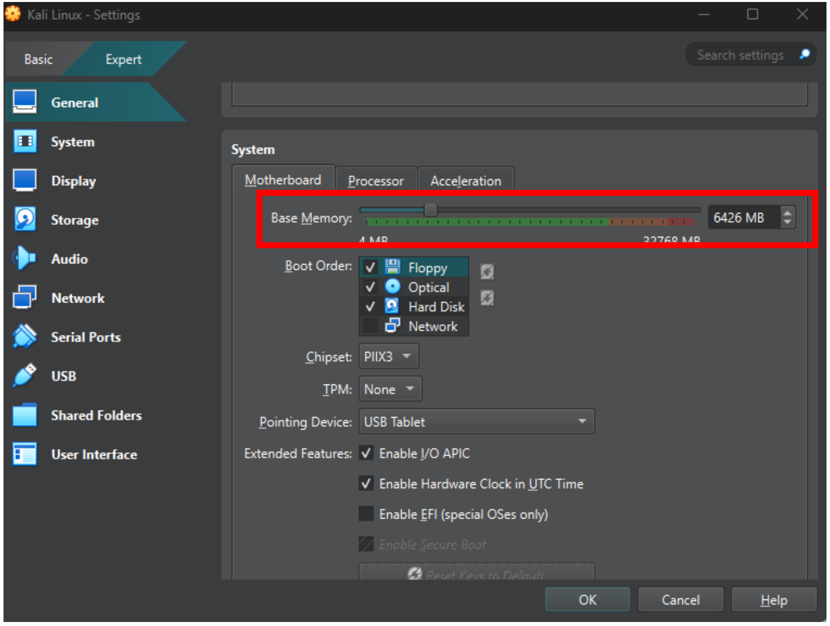
System

Base Memory: 1024 MB

4 MB 32768 MB

Boot Order: ✓ Floppy

m. In the System box, increase the Base Memory to what ever you want.



System

Base Memory: 6426 MB

4 MB 32768 MB

Boot Order: ✓ Floppy
✓ Optical
✓ Hard Disk
Network

Chipset: PIIX3

TPM: None

Pointing Device: USB Tablet

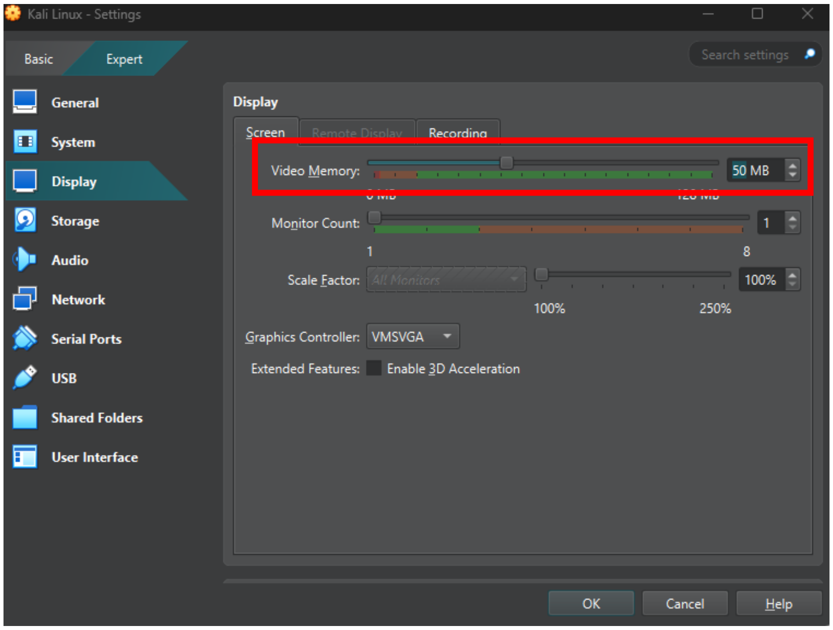
Extended Features: ✓ Enable I/O APIC

✓ Enable Hardware Clock in UTC Time

□ Enable EFI (special OSes only)

□ Enable Secure Boot

n. In the Display box, increase the Video Memory. This will decrease lag issues while running the VM.



Video Memory: 50 MB

Monitor Count: 1

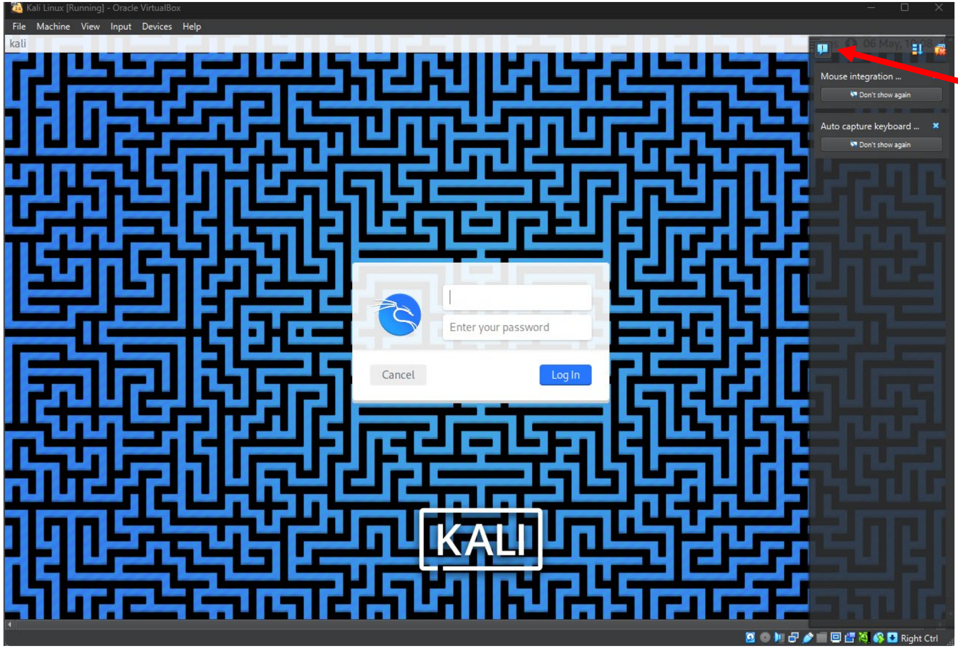
Scale Factor: All Monitors 100%

Graphics Controller: VMSVGA

Extended Features: □ Enable 3D Acceleration

o. Select OK to close the Settings window.

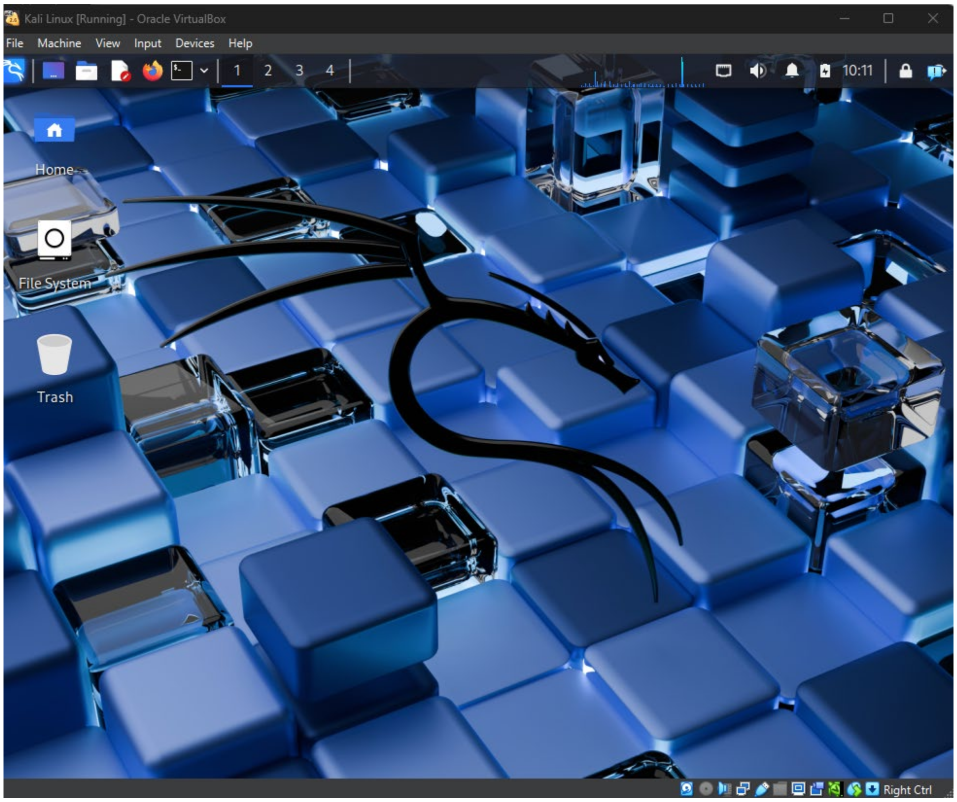
p. Select Start In the VirtualBox Manager. While the VM is loading, you will see the screen toggle. Once the VM has fully started, you will see this screen.



You can close this window by clicking on the message icon.

q. The username and password are preset to 'kali'.

r. Once logged in, your VM will look like this. You are all set for the hands-on portion of the digital forensics workshop.



s. Open the terminal. Install the required python dependencies. Run the following commands:

- sudo apt install -y python3-dev libpython3-dev python3-pip python3-setuptools python3-wheel
- python3 -m pip install -U distorm3 yara pycrypto pillow openpyxl ujson pytz ipython –break-system-packages

If you get an error, that is fine. The volatility3 framework will still work.

t. Now, clone the volatility3 source code from GitHub. Make sure you run this command while in your home directory.

- git clone https://github.com/volatilityfoundation/volatility3.git

You can verify it installed correctly with:

- python3 volatility3/vol.py -h

u. Finally, download the data and unzip the folder to the Kali Linux home directory: https://drive.google.com/file/d/1KqKK7IGun12SeSsZfEufEhVEiptVXJsI/view?usp=drive_link; password is 'infected'